NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SCRIPTING QUALITY OF SECURITY SERVICE (QoSS) SAFEGUARD MEASURES FOR THE SUGGESTED INFOCON SYSTEM

by

Jennifer Guild

March 2004

Thesis Advisor:	George W. Dinolt
Thesis Advisor:	J.D. Fulp

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Scripting Quality of Security Service (QoSS) Safeguard Measures for the suggested INFOCON System			**5. FUNDING NUMBERS**
6. AUTHOR(S) Jennifer Guild			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The existing INFOCON system is an information warning system that the DOD maintains. It is not formally correlated to other warning systems, such as DEFCON, FPCON/THREATCON, WATCHCONs, SANS INFOCON, or the Homeland Security Advisory System Threat condition. The criteria for each INFOCON level is subjective. The INFOCON recommended actions are a mix of policy and general technical measures. The INFOCON system vaguely follows the Defense in Depth network defense methodology.

This thesis examines the foundations for the existing INFOCON system and presents an evolved INFOCON system. The focus will be on the security of the DOD information infrastructure and the accomplishment of the mission, as well as the usability and the standardization of the INFOCON warning system. The end result is a prototype that is a set of predefined escalation scripts for the evolved INFOCON system's safeguard measures.

14. SUBJECT TERMS DEFCON, FPCON/THREATCON, WATCHCONs, SANS INFOCON, DOD, Defense in Depth, INFOCON, Information, Information Assurance, Actions			**15. NUMBER OF PAGES** 144
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

SCRIPTING QUALITY OF SECURITY SERVICE (QoSS) SAFEGUARD MEASURES FOR THE SUGGESTED INFOCON SYSTEM

Jennifer A. Guild
Civilian, Federal Cyber Service Corps, Naval Postgraduate School
B.S., California Lutheran University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: Jennifer A. Guild

Approved by: Dr. George W. Dinolt
Thesis Co-Advisor

J.D. Fulp
Thesis Co-Advisor

Dr. Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The existing INFOCON system is an information warning system that the DOD maintains. It is not formally correlated to other warning systems, such as DEFCON, FPCON/THREATCON, WATCHCONs, SANS INFOCON, or the Homeland Security Advisory System Threat condition. The criteria for each INFOCON level are subjective. The INFOCON recommended actions are a mix of policy and general technical measures. The INFOCON system vaguely follows the Defense in Depth network defense methodology.

This thesis examines the foundations for the existing INFOCON system and presents an evolved INFOCON system. The focus will be on the security of the DOD information infrastructure and the accomplishment of the mission, as well as the usability and the standardization of the INFOCON warning system. The end result is a prototype that is a set of predefined escalation scripts for the evolved INFOCON system's safeguard measures.

THIS PAGE INTENTIONALLY LEFT BLANK

DISCLAIMER STATEMENT

“The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.”

"This material is based upon work supported by the National Science Foundation under Grant No. DUE-0210762."

"Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.”

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND....1
B. PURPOSE OF STUDY....2
1. Scope and Assumptions....2
2. Research Questions....3
C. ORGANIZATION OF PAPER....3
1. Characterization of Existing Warning Systems....3
2. Analysis of Existing INFOCON Systems....3
3. Analysis of Network Defense Methodologies....3
4. Recommendations....3
5. Development of Safeguard Measures Scripts....4
6. Conclusions....4

II. CHARACTERIZATION OF EXISTING WARNING SYSTEMS....5
A. INFOCON....5
B. SANS INFOCON....6
C. FPCON/THREATCON....7
1. THREATCON....7
2. FPCON....7
D. HSAS THREAT CONDITIONS....9
E. DEFCON....11
F. WATCHCONS....11
1. WATCHCON....11
2. CNA-WATCHCON....12
G. RELATIONSHIPS AMONG THE WARNING SYSTEMS....12

III. ANALYSIS OF EXISTING INFOCON SYSTEM....15
A. AUTHORITY....15
B. APPLICABILITY/SCOPE....16
C. PROCEDURES....16
1. Determining the INFOCON....16
2. Declaring the INFOCON....16
D. ANALYSIS OF EACH INFOCON LEVEL CRITERIA....17
1. Normal....17
2. Alpha....17
3. Bravo....17
4. Charlie....17
5. Delta....18
6. Summary....18
E. ANALYSIS OF EACH INFOCON LEVEL'S RECOMMENDED ACTIONS....19
1. Normal....21

2. Alpha 21
3. Bravo 22
4. Charlie 22
5. Delta 22
6. Summary 23
F. ANALYSIS OF INFOCON LEVELS TO DETERMINE DEMARCATION METHOD 23
IV. ANALYSIS OF NETWORK DEFENSE METHODOLOGIES 25
A. PERIMETER DEFENSE 26
B. DETECTION METHODOLOGY 27
C. ENCRYPTION 27
D. PHYSICAL SECURITY 28
E. DEFENSE IN DEPTH METHODOLOGY 28
F. SUMMARY 30
V. RECOMMENDATIONS 31
A. LEVELS 31
1. Demarcation Method 31
2. Number of Levels 32
3. Description 32
4. Criteria 33
5. Roles and Responsibilities 36
B. SAFEGUARD MEASURES 36
C. SUMMARY 41
VI. SAFEGUARD MEASURES SCRIPTS 45
A. SCRIPT CONSIDERATIONS 45
B. PROTOTYPE NETWORK 46
C. SCRIPTS 47
1. Infocon 48
2. Gateway Router 48
3. Managed Switch 50
4. Syslog 51
D. SUMMARY 51
VII. CONCLUSIONS 53
A. CONCLUSIONS 55
B. FUTURE WORK 55
APPENDIX A – ACRONYMS 57
APPENDIX B – TERMS AND CONCEPTS 59
APPENDIX C – INFOCON ENCLOSURE (SOURCE RA02) 61
APPENDIX D – FPCON (SOURCE JO01) 83
APPENDIX E – HOMELAND SECURITY PRESIDENTIAL DIRECTIVE - 3 (SOURCE WH01) 87

APPENDIX F – INFOCON POLICY RECOMMENDED ACTIONS.....91

APPENDIX G – APACHE WEB SERVER SCRIPT.....93

APPENDIX H – GATEWAY ROUTER CONFIGURATION FILES (SOURCE CI01, FI01, KO01, NA05, RO01, ST01).....95

APPENDIX I – MANAGED SWITCH CONFIGURATION FILES (SOURCE CI01, FI01, KO01, NA05, RO01, ST01) 109

LIST OF REFERENCES.....115

INITIAL DISTRIBUTION LIST 121

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. INFOCON Levels. 6
Figure 2. FPCON Levels. 8
Figure 3. HSAS Levels. 10
Figure 4. Scope of warning systems. 12
Figure 5. Collective Stimulus of Warning Systems on the INFOCON System. 13
Figure 6. WATCHCONs influence on other warning systems. 14
Figure 7. Illustration of DID with DMZ 29
Figure 8. INFOCON Levels 33
Figure 9. Prototype Network Diagram 47
Figure 10. Flow diagram of prototype scripts 48

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Suggested INFOCON Safeguard Measures. 41

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This material is based on work supported by the national Science Foundation under Grant DUE-0210762. The preparation of this thesis would not have been possible without the technical assistance of the following great people (in alphabetical order):

• Francis Afinidad
PhD Student
Naval Postgraduate School
Monterey, California USA

• Col. Karen Burke
Computer Science Department
Naval Postgraduate School
Monterey, California USA

• Scott Cote
Computer Science Department
Naval Postgraduate School
Monterey, California USA

• Dr. George Dinolt

Computer Science Department
Naval Postgraduate School
Monterey, California USA

• Mr. J. D. Fulp
Computer Science Department
Naval Postgraduate School
Monterey, California USA

• Jim Guild
Student
Naval Postgraduate School
Monterey, California USA

• Ken Johns
Student
Naval Postgraduate School
Monterey, California USA

I wish to thank the agencies involved for allowing me the time to speak with their employees. Their ideas, thoughts and expertise greatly assisted me in this thesis effort.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The Department of Defense (DOD) commissioned research in the 1960's into developing new electromagnetic pulse (EMP) proof networking technology. The research became known as the ARPANET, because the project was funded by the Advanced Research Projects Agency. The ARPANET grew to connect military agencies, universities, and national laboratories. When the Transmission Control Protocol (TCP) and Internet Protocol (IP) were adopted for the ARPANET, several common terms were formed. An internet is a set of TCP/IP connected networks. The proper noun name Internet (with capital 'i') was coined for the ARPANET to describe the connected TCP/IP internets. [FU03, ZA01, GM01]

It wasn't until 1984 that computer viruses were seen as a potential widespread problem for the Internet. The first large-scale attack against computers connected to the Internet was the "Internet worm" that was launched in 1988. So, before the first commercial provider of Internet (not the ARPANET)[1] dial-up access went on-line in 1990, there had already been attacks against computers on the Internet. By 1995, traditional, online, dial-up services, such as America Online and Prodigy, began to provide Internet access. [FU03, ZA01, GM01]

In a report in 1996, the Defense Science Board identified a need for structured responses to attacks on the Nation's information infrastructure. That same year Information Assurance (IA) was defined as:

> Information Operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. [CN01]

Information Operations are the actions taken to affect an adversary's information and Information Systems (IS) while defending one's own information and Information Systems. [CN01, DE02]

[1] Dial up networks that provided limited access to the ARPANET were available in the 1970's.[DI02]

The Information Operations Condition (INFOCON) system was implemented in 1999. It recommends actions and raises the awareness and information assurance standards to the appropriate level of readiness to meet expected cyber threats and attacks against the DOD information infrastructure (DII). This infrastructure includes computer and telecommunications networks and systems. The INFOCON system provides a hierarchy of protection profiles that should be implemented to defend networks. [KE01, RA02]. These are not the same INFOCON levels as those from the SANS Institute.[2] [SY01]

B. PURPOSE OF STUDY

1. Scope and Assumptions

This thesis will assess the existing INFOCON levels to ascertain the specific threats indicated by each, then proceed to and define a set of security safeguards that are appropriate threat-mitigation responses for each of the threat levels. A prototype, proof-of-concept set of configuration scripts will be developed shown that effect the set of safeguards by modifying the security profile of three network/networked devices/tools (e.g., change a gateway router's filter rule-set, change the auditing granularity that the Syslog server receives, or have a switch block specific port). The groundwork laid by this thesis could potentially lead to additional research that, in turn would leads to a dynamic implementation of a Quality of Security Service (QoSS) architecture. This thesis will make no attempt to create an artificially intelligent agent that will automatically control the entire process of detecting threats and reconfiguring the network's defensive posture in real-time; nor will there be a comprehensive protection mechanism developed.

This research will define sets of network security safeguard measures that are appropriate to counter the explicit and implicit threats posed by each of the existing INFOCON threat levels. The research will develop a proof-of-concept set of configuration scripts that alter the defensive security posture of 2-3 network/networked devices/services (e.g., router, server, switch).

[2] For detailed information regarding SANS Infocon, please visit http://isc.sans.org/ (February 2004) or http://www.sans.org (February 2004).

2. Research Questions

This thesis will answer the following questions.

- **How are the INFOCON levels defined?**
  - By the perceived threat?
  - By what that threat is directed against?
  - By mitigation response measures?
- **How are the INFOCON levels demarcated?**
  - What criteria constitutes the "cutoff" between each layer?
  - Is there a common "theme" to each layer that could be leveraged when choosing the appropriate set of safeguard techniques to apply?
- **What is the current landscape of network defense methodologies?**
  - Is it predominantly ad-hoc, or is there a pre-defined escalation approach?
  - What defense mechanisms, if any, lend themselves to an automated invocation and/or re-configuration?
- **What is the appropriate tactical response to each of the INFOCON levels?**
- **What security-implementing devices/services would make good candidates for implementing the security scripts?**
- **Can the safeguard scripts be centrally managed?**

C. ORGANIZATION OF PAPER

1. Characterization of Existing Warning Systems

Some of the existing warning systems and their relationship to each other and the INFOCON system will be discussed.

2. Analysis of Existing INFOCON Systems

The INFOCON levels will be analyzed to characterize each level and determine the method of demarcation. The relationship among some of the existing warning systems, to include the INFOCON, will also be analyzed.

3. Analysis of Network Defense Methodologies

Defense methodologies currently in existence will be analyzed with particular emphasis being given to those methodologies specific to the DOD.

4. Recommendations

Define an evolutionary INFOCON system that satisfies the goal of the existing INFOCON system. The new INFOCON system should improve usability, feasibility, and the security of the DOD information infrastructure. The safeguard measures that are presented should be specific, technical, and feasible. The measures will be roughly

categorized by their functional area. In each area, the safeguard measures will be mapped to the devices/tools which will implement them. The criteria for selecting the prototype devices/tools will be discussed. The devices will include a gateway router, a managed switch, and a Syslog server.

5. Development of Safeguard Measures Scripts

For each device/service, a safeguard script will be developed for each of the suggested INFOCON threat levels that effects the suggested safeguard measures for that level.

6. Conclusions

Summarize the evolved INFOCON system and its benefits. Present the conclusions, including the feasibility of the evolved system and any future work. The research questions will be answered.

II. CHARACTERIZATION OF EXISTING WARNING SYSTEMS

There are many warning systems in existence in the United States and the world. Most of these were created and used by United States Government organizations. The information revolution has caused the corporate sector to create their own information warning systems as well. This chapter will only cover those systems that should directly relate to, or influence, the protection of information that falls under the purview of the U.S. Government; with an added focus on DOD-specific warning systems. [AD01, FA01, FA02, RA01, RA02, US01, WE01]

A. INFOCON

The INFOCON system is a defensive warning system for the DOD based on military operations, the intelligence assessment of adversary capabilities and intent, information network indicators, and the status of information systems.[3] It is a system of progressive levels of the probability of attack and its impact to military operations. The corresponding response measures are mostly reactionary. They are meant to include preventive actions, reactive actions taken during an attack, and mitigating, damage control actions. Reactive actions during the attack would be those to stop an attack, where as mitigating actions are actions to limit or reverse damage to the system. [LU01, OF01, RA01, RA02, US01, WE01]

There are five INFOCON levels. The range from lowest to highest is Normal through Delta. Each level has criteria. One or more of the criterion of that level must be met to substanstiate a change to that level. The criteria for each level are broad guidance to consider, not firm rules. Also, each level has recommended actions, which are the response measures to the expected threat. The system is maintained by the Joint Task Force for Computer Network Operations (JTF-CNO). The criteria, recommended actions, authority, applicability, and procedures are detailed further in Chapter 3. [LU01, OF01, RA01, RA02, US01]

[3]For more information please visit http://207.133.209.84/amc/ci/matrix/documents/cjcs_level/cjcs-infocon.pdf February 2004.

Figure 1. INFOCON Levels.

B. SANS INFOCON

The SysAdmin, Audit, Network, Security (SANS) Institute maintains its own INFOCON system in conjunction with its Internet Storm Center.[4] This system is intended to indicate the condition of the Internet infrastructure, not monitor particular nations or companies.[5] It reflects changes in malicious traffic and the possibility of connectivity disruption. [SANS00]

There are four levels in this system, indicated by color. The lowest level is green, indicating and the situation is normal with no known threats. The next level is yellow, indicating that SANS is tracking a significant new threat whose impact is not known or is expected to be minor to the Internet infrastructure. At this level, SANS advises users to take immediate action to contain the impact. Orange is the next level and indicates that a major disruption in Internet connectivity is imminent or in progress, but there is no action specified by SANS. The highest level, red, indicates a loss of connectivity across a large part of the Internet infrastructure, but again, with no remedial action specified by SANS. [SANS00]

[4] For detailed information regarding SANS Infocon, please visit http://isc.sans.org/ (February 2004) or http://www.sans.org (February 2004)

[5] For information regarding the authority, applicability, and procedures please visit http://isc.sans.org/about.html (February 2004)

C. FPCON/THREATCON

1. THREATCON

THREATCON is the acronym for the terrorist threat condition.[6] It is a standardized system of threat conditions that describes five progressive levels of protective measures implemented by the DOD in response to terrorist threats to all U.S. Military personnel and facilities. This is not the ThreatCon as defined by Symantec Corporation. Because of the confusion with the Department of State's Threat Levels, the name THREATCON was replaced by FPCON in Jun 2001. [AD01, AN01, DI01, DOD02, EU01, FA01, ST03, US01, US02, WE01]

2. FPCON

FPCON is the acronym for the force protection condition. Though the name changed from THREATCON, the system, individual classifications and measures remain the same.[7][8] The FPCON system has five levels. Incidentally, the levels have the same names as the INFOCON levels. The levels are Normal, Alpha, Bravo, Charlie, and Delta. The measures for the levels, also like the INFOCON level recommended actions, build upon the prior level. [AN01, DI01, DOD02, DT02, EU01, FA01, ST03, US01, US02, WE01]

---

6 For more details: http://www.fas.org/irp/doddir/dod/app-J_THREATCON.htm (February 2004)

7 Please see http://www.angelfire.com/ca7/Security/threatcon.html (February 2004) for more details

8 Please see http://www.dtic.mil/whs/directives/corres/pdf/d200012_081803/d200012p.pdf (February 2004) for more details on applicability, authority, and procedures.

Figure 2. FPCON Levels.

The FPCON Normal level is indicated when there is no discernable terrorist activity. Because there always exists a general threat of possible terrorist activity, a routine security posture is warranted. Its recommended actions are to secure areas when not in use, maintain positive control of identification, and be aware of local anti-government demonstrations. [AN01, EU01, DOD02, FA01, JO01, ST03, US02, WE01]

If the threat of terrorist attack is low, meaning there are general, nonspecific threats of terrorist activity against personnel and/or facilities of unpredictable nature and unknown extent, then FPCON level Alpha is indicated. This level must be maintainable indefinitely with only limited impact on operations. Though the circumstances don't justify full implementation of FPCON Bravo, it may be necessary to implement certain measures from higher FPCON levels as a deterrent or because of intelligence received. See Appendix D, FPCON, for the complete listing of recommended actions for this level. [AN01, EU01, DOD02, FA01, JO01, ST03, US02, WE01]

FPCON Bravo is indicated when an increased and more predictable threat of terrorist activity exists, but no specific threat has been identified. This level's recommended measures must be maintainable for several weeks without substantially affecting operational capabilities, causing undue hardship to personnel, or aggravating relations with local authorities, members of the local civilian, or host nation community.

See Appendix D, FPCON, for the complete listing of recommended actions for this level. [AN01, EU01, DOD02, FA01, JO01, ST03, US02, WE01]

The next level, FPCON Charlie, is indicated when intelligence indicates that a threat action against personnel and facilities is imminent or an incident has occurred. If Charlie's recommended measures are implemented for more than a short duration, then hardships will probably be created and peacetime activities for personnel and units will be affected. [AN01, EU01, DOD02, FA01, JO01, ST03, US02, WE01]

Finally, FPCON Delta is indicated in the immediate area when intelligence indicates terrorist action against a specific location or person is likely or when a threat attack has occurred. The implementation of FPCON Delta is normally for only limited duration over specific, localized areas. This condition will cause significant personnel hardships and substantial peacetime mission capability reduction if sustained for extended durations. [AN01, EU01, DOD02, FA01, JO01, ST03, US02, WE01]

D. HSAS THREAT CONDITIONS

The Homeland Security Advisory System, HSAS, is a product of the newly formed Department of Homeland Security (DHS).[9] It provides a nationwide, comprehensive, effective means of disseminating information regarding the risk of terrorist acts. It provides warnings using the graduated Threat Conditions, which that increase as the risk of the threat increases. Each Threat Condition has a corresponding set of Protective Measures. These Protective Measures are in addition to each agency's or department's specific measures. Federal agencies and departments implement the corresponding Protective Measures to best reduce their vulnerability or increase their response capability for the indicated threat level. The Threat Conditions are assigned by the Attorney General of the United States of America in consultation with the Assistant to the President for Homeland Security. The DHS directive that describes the HSAS may be found in Appendix E, Homeland Security Advisory System.[10] [WH01]

[9] For more information, see http://www.dhs.gov/dhspublic/ (February 2004)

[10] The authority, applicability, and procedures for the HSAS Threatcon can be found in Appendix E.

Figure 3. HSAS Levels.

There are also five HSAS Threat Conditions. Higher threat conditions indicate both a higher likelihood of attack, in addition to an expectation of greater severity per attack. Each Threat Condition is identified by a descriptor and corresponding color. [WH01]

The lowest Threat Condition is Low, which is represented by the color green. It is declared when there is a low risk of terrorist attacks. The next level is Guarded and it is represented by the color blue. The Guarded condition is declared when there is a general risk of terrorist attacks. It is followed by Elevated, which is represented by the color yellow. This condition is declared when there is a significant risk of terrorist attacks. The level High, is the second highest level .and is represent by the color orange. A High condition is declared when there is a high risk of terrorist attacks. Finally, the highest level, Severe, is represented by the color red. It reflects a severe risk of terrorist attacks. This level's protective measures aren't intended to be sustained for substantial durations of time. [WH01]

E. DEFCON

DEFCON is the acronym for Defense Readiness Condition. This system describes progressive alert postures, which are primarily used by the Joint Chiefs of Staff and the commanders of unified commands.[11] These conditions are phased increases in combat readiness. They are graduated to match situations of varying military severity. [FA02, SC01, ST03]

There are five DEFCON levels, from 1 to 5. The lowest is DEFCON 5, which is normal, peacetime readiness. DEFCON 4 is normal, peacetime readiness, but with increased intelligence and strengthened security measures. An increase in force readiness above normal readiness is implemented at DEFCON 3. A further increase in force readiness that is less than the maximum readiness is set at DEFCON 2. The maximum force readiness is DEFCON 1. [FA02, SC01, ST03]

F. WATCHCONS

These are classified warning systems from the intelligence communities.[12] These systems will only receive cursory coverage here due to the classified nature of their domain. Both systems have five levels. The level descriptions are 1 to 5. WATCHCON 5 is normal conditions without any unusual military movements. Level 4 of the WATCHCON is normal conditions with a potential threat that requires continued surveillance. There is a concern for an increased threat against the national security at WATCHCON 3. Signs of eminent danger and significant threat to national interest are WATCHCON 2. WATCHCON 1 is a clear immediate threat of enemy attack. [GL01, IE01, KE01, KE02]

1. WATCHCON

The Watch Condition, or WATCHCON, system is a defensive warning system based on the intelligence community's degree of concern regarding a particular warning issue. [KE01, KE02, RA02]

---

[11] Please see http://www.fas.org/nuke/guide/usa/c3i/defcon.htm (February 2004) for more information for more information. Minimal information found on authority, applicability, and procedures.

[12] No information could be found regarding the authority, applicability, and procedures for the WATCHCONs.

2. CNA-WATCHCON

The Computer Network Attack Watch Condition, or CNA-WATCHCON, system is another warning system based on assessment of intelligence that includes the overall political situation and the CNA threat levels. [KE01, KE02, RA02]

G. RELATIONSHIPS AMONG THE WARNING SYSTEMS

Each of the systems discussed, are systems currently in use in the United States. The FPCON levels represent the defensive condition of the United States military and its assets abroad. The Homeland Security Advisory System represents the preparedness and readiness of the United States against the terrorist threat. The DEFCON levels represent the United States' military preparedness for the likelihood of war. The WATCHCONs represent the intelligence community's concern regarding a specific problem in the world. The SANS INFOCON represents the condition of the world's Internet infrastructure. The INFOCON levels represent the United States Department of Defense's preparedness and readiness for the intentional disruption of DOD information systems. [FA02, NA02, NA04, RA01, RA02, SC01, WE01]

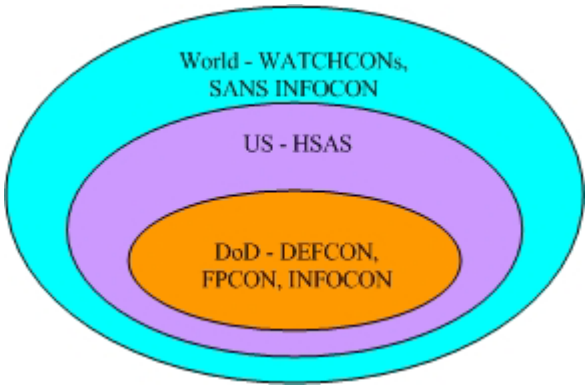

Figure 4. Scope of warning systems.

All of the systems are roughly analogous. Each is defined by one or more combinations of: an assessed threat, the capability to implement the necessary protective measures, and the overall risk to the organizations.

Does one system influence another? It would be assumed that each affects the others because all of the systems relate to very broad factors that contribute to the all-

around defensive preparedness of the United States. Thus, all of the more general coverage warning systems should have some form of impact on the more specific INFOCON level: more specific because it addresses threats specifically to information. The inverse does not hold true; i.e., the INFOCON level would not always be expected to influence the other systems. This because some of the other warning systems are focused on their specific task and the INFOCON doesn't fall into that task. This thesis is interested in what drives the INFOCON level, so as to better define the appropriate measures for each level. [FA02, NA02, RA01, RA02, SC01, WE01]

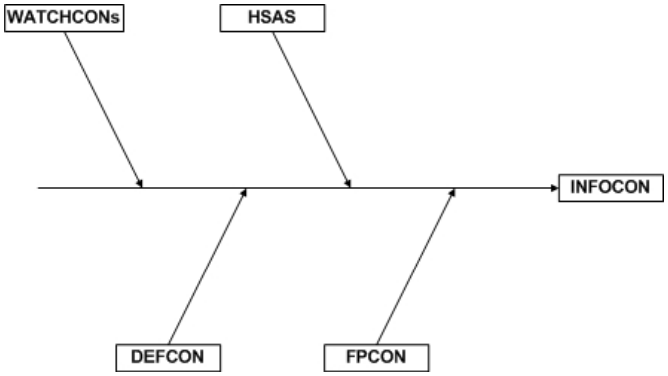

Figure 5. Collective Stimulus of Warning Systems on the INFOCON System.

The FPCON and HSAS Threat Condition levels are both defined by terrorist threats and activity, which that should link the two systems closely together. Also, because the HSAS is nationwide and the FPCON is a DOD warning system, HSAS should influence the FPCON level. Or, the FPCON should influence the HSAS because the FPCON level covers the US and its assets aboard while HSAS only covers the US. Neither seems to be the case.

The original INFOCON documentation states that the THREATCON, now FPCON, may impact the INFOCON level. Currently, the JTF-CNO doesn't suggest that either the FPCON or the HSAS impact the INFOCON. This may be because terrorists haven't, as far as we know, yet resorted to cyber terrorism.

The FPCON and DEFCON systems are both indicators of the world situation. The DEFCON levels represent our likelihood of going to war. This is one system that

should influence the INFOCON level, because if war is imminent or occurring our information systems should employ greater protective measures in expectation that the enemy will be targeting them with any means at their disposal. Though, at DEFCON 1, there may be some situations that require no addition protective measures be in place in order to accomplish the mission. The original INFOCON document states that DEFCON may impact the INFOCON level. However, the JTF-CNO discourages correlation between the DEFCON level and the INFOCON level. [ST02]

There is no correlation between any of the governmental warning systems and the SANS INFOCON system.

The intelligence community's level of concern, which is represented by WATCHCON and CNA-WATCHCON systems, seems to be the one warning system that has a direct correlation to the INFOCON. Intelligence assessments from the WATCHCONs are in the criteria for the INFOCON levels. In fact, the WATCHCONs seem to have influence on all of other the warning systems. This makes sense, because all of the warning systems have an intelligence assessment component.

This relationship among the various threat systems is presented in Figure 6. This figure highlights both the comprehensive coverage of the WATCHCON systems, in addition to the overlapping, cross-influential relationships among the remaining systems. Of particular import to this thesis is the notion that the INFOCON levels are influenced to some degree by the Nation's other governmental threat level systems.

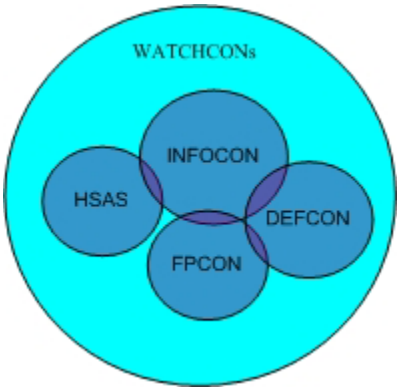

Figure 6. WATCHCONs influence on other warning systems.

III. ANALYSIS OF EXISTING INFOCON SYSTEM

Before analyzing the INFOCON System, the four assumptions made by its drafters should be presented. These assumptions are explicitly expressed as such in the original INFOCON documentation. First among these assumptions is the belief that a successful intrusion in one network may facilitate access to another network, so it is assumed that a risk assumed by one is a risk that may eventually be "shared" by all. The methods employed by increasingly more sophisticated attackers are more problematic to detect. Thus, it is another assumption that the protective measures must be planned, exercised, and executed in advance of an attack. That the anonymous nature of an attacker must not hinder the execution of defensive strategies and tactics is another assumption. Similarly; that an incident that could be an attack, system anomaly, or operator error, should be characterized as malicious until assessed otherwise is the final assumption. [LU01, OF01, RA02]

There are several places that indications and warning are mentioned in the criteria. These are the indications and warning for Information Operations from the CNA-WATCHCON. CNA intelligence assessments, specific criteria, and procedures are classified SECRET or higher, so no further detail about them will be discussed in this thesis.. [DE03, RA02]

The purpose of the INFOCON is to recommend actions that uniformly heighten or reduce the DOD defensive posture, to defend against CNA, and to mitigate sustained damage to the DOD information infrastructure. There are five INFOCON levels. The range from lowest to highest is Normal through Delta. Each level has criteria. Any of the level's criterion can be met to justify elevation to that level. The criteria for each level are broad guidance to consider, not firm rules. [LU01, OF01, RA02]

A. AUTHORITY

This system was established by the Secretary of Defense. Initially, it was administered through the Director for Operations, Joint Staff (J-3). It is currently

administered by the Commander, Joint Task Force for Computer Network Defense (JTF-CND). The JTF-CNO is the office that is currently tasked with updating/reworking the INFOCON system.

B. APPLICABILITY/SCOPE

The INFOCON system is used throughout the Department of Defense, all over the world. This includes the Joint Staff, Services, combatant commands, and Defense agencies. The INFOCON system applies in both peacetime and war. All commands and support agencies must develop procedures specific to their command/agency in addition to those already recommended. Procedures developed are propagated downwards. [RA02]

C. PROCEDURES

There are two sets of procedures to consider. *Why* the INFOCON level changes is in the procedures on how to determine the INFOCON level, and *Who* can make changes to the INFOCON level is in the procedures for declaring the INFOCON level.

1. Determining the INFOCON

The INFOCON level is based on significant changes to operational, technical, and/or intelligence factors. These factors are further detailed in Section 3-D, the analysis of the criteria. The JTF-CNO assimilates and evaluates information to assess the CND situation DOD-wide. Commanders must assess the situation and establish the proper INFOCON based on the evaluation of all relevant factors. [RA02]

2. Declaring the INFOCON

The INFOCON is set for the DOD by the Secretary of Defense (SecDef). The JTF-CNO recommends the changes through the Chairman of the Joint Chiefs of Staff (CJCS) to the SecDef, who may further delegate declaration authority to the JTF-CND. All commands and agencies may change their organization's INFOCON level, but they must remain at an INFOCON level that is no less than the INFOCON directed by SecDef or the CJCS. [RA02]

D. ANALYSIS OF EACH INFOCON LEVEL CRITERIA

1. Normal

The lowest INFOCON level is Normal and it indicates normal activity. The only criteria for maintaining this level is that there is no significant probability of attack against the network. The existing INFOCON doesn't require a specific tools or devices to secure the network. [LU01, RA02]

2. Alpha

The next level, Alpha, indicates an increased probability of attack. The primary consideration, per the JTF-CND, is to consider if there is any planned or ongoing military operation, contingency or exercise that requires increased security of information systems. The next, item to consider is if whether the CNA intelligence indications and warnings (I&W) indicate a general threat. Any detected network scans, probes, or other activities indicating a pattern of surveillance would be the next consideration. Regional events that affect US interests and that involve potential adversaries with suspected or known CNA capability would be the final indication to elevate to the Alpha level. [LU01, RA02]

3. Bravo

The Bravo level indicates a specific probability of attack. A planned or ongoing major military operation or contingency would be the first criteria to consider. This would be followed by any CNA intelligence I&W indicating the specific targeting of systems, locations, units, or operations. The network consideration would be a significant level of network probes, scans, or activities detected indicating a pattern of concentrated reconnaissance activities. The final consideration would be any attempted network penetration or Denial of Service (DoS) that has no current or expected impact on DOD operations. [LU01, RA02]

4. Charlie

The occurrence of limited attacks indicates Charlie level. There are two main criteria. The intelligence assessment(s) indicating a limited attack is the proactive criterion. The other criterion is the detected attack(s) on information systems with limited impact to DOD operations. Limited impact is defined as minimal success of the

attacker and the attack successfully counteracted, little or no data or systems compromised, or the unit is able to accomplish its mission. [LU01, RA02]

5. Delta

The highest level, Delta, indicates the occurrence of general attacks. It has two criterion to consider, both of which have to do with the impact of incidents. The detected, successful attack(s) on information systems that impact DOD operations is one criterion. The other is widespread incidents that undermine the ability of the unit to function effectively causing a significant risk of mission failure. [LU01, RA02]

6. Summary

At each level there are four considerations to be taken in order of increasing significance per the JTF-CNO. First, any planned or ongoing military operation(s) is the criterion with the greatest significance. Any intelligence I&W is the next consideration in significance. Detected network activities indicating reconnaissance or attack is the second lowest item of significance. Interestingly, the impact of a CNA is the least significant criterion, but it is the only criterion for the highest INFOCON level. [LU01, RA02]

These four considerations fall into three broad categories of or factors that influence the INFOCON level. These categories are operational, technical, and intelligence. The intelligence category includes such areas as US CNA intelligence, foreign intelligence, and law enforcement intelligence. Significant changes in one or more of the three categories is the basis for the INFOCON level. [LU01, RA02]

An increase in the probability of an attack is reflected by each level, culminating in the Delta level, which requires the occurrence of general attacks. The probability of an attack would be derived from the combination of actual events and expected events. Thus, the probability of an attack is one possible, implied method of definition for the criteria. [LU01, RA02]

The severity of impact of the attack also increases with each level, to the point that it is the only criteria for the Delta level. Though the impact is considered the least significant criterion, it is still a contributing element to the definition of the INFOCON

level criteria. Therefore, another possible, implied method of definition for the criteria is the severity of the impact of the threat or attack. [LU01, RA02]

The documentation does not give an explicit definition nor is there definitive evidence that there is a definition. The analysis of the INFOCON level criteria revealed two possible implied definitions from the vague, generalized criteria, which are the severity of the impact of the attack and the probability of an attack. Therefore, in the absence of concrete criteria or definitions, the probability of an attack and the severity of the impact of an attack are the implied methods of definition selected for the INFOCON levels.

E. ANALYSIS OF EACH INFOCON LEVEL'S RECOMMENDED ACTIONS

The recommended actions include some 'appropriate' general security practices, which are detailed below. These very general security practices, which, if implemented correctly, can significantly reduce the risk of a successful attack against an information system. Good, solid security practices are the foundation of a sound, prevention-based, information assurance program. The next several paragraphs detail some of the conceptual security practices as put forth by the INFOCON guidelines. [RA02]

System administration, including system security administration, is always critical to securing an information system. Organizations must ensure their systems are administered by technically qualified and experienced personnel. These personnel must be provided periodic professional training in system administration and security. All system administrators (SAs) and system security administrators (SSAs) require the necessary tools to assist them in effective baseline management, auditing, and network intrusion detection. Also, critical to reliable and secure operations are configuration management, proper staffing, and strong systems security policies. [RA02]

SAs should perform regular auditing and log review for suspicious activity. Logging and review requirements should increase as the INFOCON level increases. These requirements include more frequent reviews, analysis of activity below normal trigger thresholds, focused string searches, and the submission of logs to a designated organization that conducts specialized reviews. [RA02]

Periodic back-ups of files critical to the accomplishment of the mission should be conducted by the system administrators. The storage of the back-ups should be isolated from any network, as well as, physically separated from the originating facility. A rise in the INFOCON level may warrant an increase in the frequency of back-ups, but there are no guidelines specified. If the INFOCON level increases, back-up frequency may increase from quarterly, monthly, or weekly to daily or real-time. [RA02]

All organizations should establish procedures for conducting internal security reviews. As a minimum, an internal security review should include; searching for default and weak passwords, conducting vulnerability scans, identifying network access points and their operational importance, raising awareness level of all users of any new vulnerabilities that are found, examination of historically dormant or infrequently used accounts for signs of unusual activity, and a review of all pertinent technical advisories. Technical advisories include the installation of patches, implementation of fixes, and the execution of preventive or mitigating actions. [RA02]

Procedures should also be established for coordinating external vulnerability assessments and analysis of the organization's information systems. Outside agencies such as DISA, NSA, and Service CERTs/CIRTs should conduct the assessments and analysis. Network scans, OPSEC surveys, COMSEC reviews, and red team operations may be included is such assessments. [RA02]

Before implementing a higher action, all actions required at the lower levels must be implemented. The appropriate general security practices that were just detailed are referred to by the documentation by two descriptions in the recommended actions of the INFOCON system. The documentation refers to appropriate response actions and appropriate security practices in different levels as recommended actions. These two descriptions seem to entail the same actions, such as increased level of auditing. This thesis will use the appropriate response actions, because appropriate security practices implies actions done on a continual basis not as a response to an indicator. There are recommended actions for each INFOCON level. Before implementing a higher action, all actions required at the lower levels must be implemented.

The recommended actions, unless specifically directed by Secretary of Defense, are the response measures associated with the INFOCON levels. The response measures must be applied judiciously, otherwise they may result in the needless loss of operational capability due to the unnecessary or overzealous application of safeguards. Such overwrought reactions might actually contribute to the adversary's objectives. Also, the response measures directed by combatant commands will take precedence over those directed by the Service INFOCONs. [RA02]

1. Normal

The Normal level's recommended actions are the minimum set of actions for all the INFOCON levels. These actions correspond to those required by any system that has been certified and accredited through the DOD Information Technology Security Certification and Accreditation Process (DITSCAP). [BU01, DI03, DOD05]

The actions at this level involve identifying all mission critical information, information systems, the information systems' operational importance, all points of access, and operation necessity of those access points. Employing normal reporting procedures, periodically reviewing and testing higher INFOCON levels, and conducting all normal security practices on a continuing basis are also recommended actions at this level. Normal security practices include conducting education and training for users, administrators, and management, conducting periodic internal security reviews, external vulnerability assessments, normal auditing, review of file back-up procedures, installing patches for newly identified vulnerabilities, and ensuring that an effective password management program is in place. [DOD04, RA01, RA02]

2. Alpha

Alpha's recommended actions are to execute appropriate response actions, and employ normal reporting procedures. Also, in addition to reviewing and testing the higher level INFOCON actions, proactive execution of those levels should be considered. Appropriate security practices at this level include increasing the level of auditing, reviewing of critical file back-up procedures, conducting internal security reviews on all critical systems, executing appropriate defensive tactics, and heightening the awareness of all information system users and administrators. [RA02]

3. Bravo

The Bravo level actions are to ensure increased reporting requirements are met, appropriate security practices are executed, as well as to, review, test, and consider proactive execution of higher level INFOCON actions. Appropriate response actions at this level include increasing the level of auditing, reviewing critical file back-up procedures, conducting immediate internal security review on all critical systems, executing appropriate defensive tactics, identifying new vulnerabilities, installing patches, and disconnecting unclassified dial-up connections not required for current operations. [RA02]

4. Charlie

The actions at Charlie level involve executing appropriate response actions, ensure increased reporting requirements are met, as well as, review, test, and consider proactive execution of higher level INFOCON actions. Appropriate response actions include conducting the maximum level of auditing, reviewing critical file back-up procedures, giving consideration to restricting traffic to mission essential communication only, reconfiguring information systems to minimize access points and increase security, re-routing mission-critical communications through unaffected systems, executing appropriate defensive tactics, employing alternative modes of communication, disseminating new contact information, and disconnecting all non-mission critical networks.

5. Delta

At Delta, the recommended actions are to ensure increased reporting requirements are met and to execute applicable portions of the continuity of operations plan. The continuity of operations plan should include isolating compromised systems from the rest of the network, designating alternate information systems, disseminating new communication procedures, executing procedures for ensuring a graceful degradation of information systems, implementing procedures for conducting operations manually or in "stand-alone" mode, and executing other appropriate defensive tactics. [RA02]

Appropriate defensive tactics at this level are the possible responses to malicious activities. Such activities may be classified into six categories. These categories are reconnaissance or suspicious activity, unauthorized access, denial of service, data

browsing, data corruption, and malicious code. Careful consideration must be given to the potential practical and legal consequences prior to the defensive tactics being executed. The defensive tactics are reactive responses to an assessed network attack. [RA02]

6. Summary

Network defense should, ideally, be based on advanced warning of a network attack occurring. The response measures should be commensurate with the risk and the mission requirements. The recommended actions as detailed above, which are quite vague, are increasingly more reactive and less preventive as the INFOCON levels escalate. Though not apparent by the very general recommended actions delineated above, it is operationally infeasible for the entire DOD to raise the INFOCON level to Bravo or above per the JTF-CND. [RA02]

F. ANALYSIS OF INFOCON LEVELS TO DETERMINE DEMARCATION METHOD

Now that the INFOCON levels have at least implied definitions, their demarcation if any, must be determined. There is no explicit demarcation method specified in the documentation. The criteria that constitute the "cutoff" between each layer needs to be determined, if there is any. The question is: Is there a common "theme" to each layer that could be leveraged when choosing the appropriate set of safeguard techniques to apply? The analysis below will consider options to determine if there are implied methods of demarcation.

The probability of an attack at the lowest level, Normal, is not significant. The next level, Alpha, indicates an increased probability of attack. Whereas, the Bravo level indicates the specific probability of attack, but successful attacks haven't occurred yet. Once limited attacks start to occur, an increase to INFOCON level Charlie is warranted. The highest level, Delta, indicates the highest probability of attack because of the actual occurrence of general attacks. [RA01, RA02]

There are several methods of demarcation that were considered based upon the authors experience and education. The INFOCON system is generalized so that those in

authority were not bound to concrete guidelines. Each INFOCON level reflects the appropriate information operation measures to be taken based on the risk posed by the intentional disruption of DOD systems. The implied demarcation method is probability of an attack because it is based on operational, intelligence, and technical information. [NA02]

This chapter has detailed the INFOCON System. The criteria used to "set" the appropriate level were shown to be very general, and without to any specific threat or even category of threat. The "appropriate security practices" are likewise quite general, as were the recommended actions. Because of this, only implied criteria of demarcation could be considered and analyzed. Without an explicit method of demarcation, the analysis needed to determine the appropriate proactive safeguard responses for each INFOCON level will also be somewhat subjective.

IV. ANALYSIS OF NETWORK DEFENSE METHODOLOGIES

The extent of the Nation's cyber vulnerability will never truly be known, because the most costly and damaging attacks are not made public. This information is generally not made public in order to preserve the integrity of public institutions. The FBI Computer Security Institute's (CSI) Computer Crime and Security Survey in 2001 stated that 85 percent of the respondents detected computer security breaches within the last 12 months. Their Internet connection was the most frequent, 70 percent, point of attack. In 2003, the Computer Crime and Security Survey found that 92 percent of the respondents had detected attacks within the last 12 months. Again, the respondents' Internet connections were the point of attack 78 percent of the time. The Nation's defense networks and computers use many of the same hardware and software as the general public. The military refers to these products as COTS, or Commercial off the Shelf products. Thus, the defense systems are subject to the same attacks as those systems. A General Accounting Office (GAO) report released in 2001, indicated that more than 60 percent of military computers had been compromised. [BU01, CO02, CSRC01, CSRC03, NA01, SANS05, SANS08, SANS10]

Though the world is at great risk from cyber attacks, there is an extraordinarily small amount research on building truly secure systems is being conducted. Only a tiny group of researchers are exploring long-term solutions to this problem. The Naval Postgraduate School Center for Information Systems Security Studies and Research (NPS CISR) lead by Dr. Cynthia Irvine, is one such group. [CI02, NA01]

Unfortunately, because of a lack of widespread knowledge on how to build secure computer systems, as well as the lack of economic impetus to build them, other methods must be employed to secure our cyber interests. The INFOCON guidance does not explicitly specify a defensive methodology that should be used. All information assurance defensive methodologies must be based on policies that are endorsed by management and that are well written, maintained, and implemented. [CL01, IR01, NA01]

A. PERIMETER DEFENSE

The perimeter defense model uses hardware and/or software to protect a network by providing well protected gateways between trusted and un-trusted network domains. It provides an "outer ring of protection" for systems in the trusted domain so that they can connect to un-trusted domains despite the presence of exploitable vulnerabilities within each of the individual systems. It is now common to see "enclaves" hiding from the Internet behind firewalls. However, these enclaves often have few native/on-board defensive measures of their own for self-protection. Most of the commercially available operating systems and networks available today only offer weak defensive mechanisms, therefore they are vulnerable and difficult to protect. [CSRC01, DE03, DT01, NA01, NA02, SC01]

General acceptance of the perimeter defense model occurred because it seemed to be easier and less expensive to secure only the gateways rather than the many applications and systems that "sit" behind them. Perimeter defenses can prevent, absorb, or detect scans, probes, or malicious attacks, thus reducing the risk to the internal network. The major risk of relying solely on a perimeter-style defensive strategy is that a single successful penetration could compromise the entire network. [CSRC01, DE03, DT01, FU01, NA01, NA02, SC01]

Typical perimeter defenses include technologies like routers, firewalls, and application proxies. There are many possible perimeter defense designs. Factors that influence design include the degree of security required and the cost. A firewall is effective at controlling external access. It also can indicate the amount and type of hostile intention the network is attracting. [DE03, FU01, SC01, ZE01]

Even though properly configured and maintained perimeter defense mechanisms prevent many types of malicious access, they do not provide protection against all outside threats. Through security flaws, adversaries directly attack user computers through email and web browsing scripting languages. [FU01, CSRC01]

B. DETECTION METHODOLOGY

Due to the large number of network security threats, it is not a matter of whether malicious activity will occur, but when and where. The Detection Methodology allows for the detection of malicious activity. Detection mechanisms identify and alert on unauthorized activity. The activity can be from an external or internal source. This is critical to security for two reasons. First, if an unauthorized person is accurately detected on a network it is possible to stop them before than can do any damage. Second, even if damage is done, it can be detected more quickly and thus facilitate prompt damage mitigating actions. [CSRC02, CSRC06, FU01, IN01, OM01, SANS08, ZD01]

The most common Detection tool is an Intrusion Detection System or IDS. IDSs can be either hardware- or software-based. It may detect security violations that can not be prevented and documents intrusion attempts to the organization. Two other detection tools are Honey Pots and Padded Cell Systems. Honey Pots are decoy systems that attempt to lure a malicious person away from the real (i.e., operational) target network. Padded Cell Systems are similar to Honey Pots, but instead of luring the malicious person, the malicious person is seamlessly transferred to a decoy system after detection. [CSRC02, CSRC06, FU01, IN01, OM01, SANS08]

The effectiveness of Detection mechanisms is based on detection accuracy and performance. The accuracy of detection is determined by the methodology employed. Performance is the mechanism's ability to reliably inspect all the traffic crossing the network. Most Detection mechanisms have several limitations. They do not scale well. They create a large number of false positives and an incredibly large volume of information. The automated systems are not usually effective against sophisticated adversaries. Finally, these mechanisms are not well protected from malicious activity themselves. [CSRC02, FU01, IN01, OM01, PR01]

C. ENCRYPTION

Encryption is the process of converting data into a form that is unreadable by anyone except the intended recipient. Encryption mechanisms can secure data on systems, as well as data that is in transit between systems or networks. Data integrity,

authentication, confidentiality, and authorization mechanisms all employ encryption to secure a system or network. [DI02, FU01, HA01, SE01, SS01]

Tools that use encryption include Virtual Private Networks (VPNs) and digital signatures. A VPN is comprised of two or more remote locations that use encrypted tunnels to create a "private" channel over a public network. Digital signatures use public key encryption techniques to ensure that a document is authentic and has not been modified. [FU01, HA01, SE01, SS01, WA01]

Encryption frequently impacts performance because of the time needed to encrypt and decrypt the data. Key management can be the weakness of encryption, because users are unwilling or unable to manage encryption keys in a secure, diligent manner. Encryption is an excellent defensive methodology, but it is not an end-all solution to security. [DA01, FU01, HA01, SE01]

D. PHYSICAL SECURITY

Not everyone considers physical security as a network defense methodology. However, unauthorized physical access to facilities defeats most of the more technical security measures of systems and networks. Therefore, it must be a primary network defense methodology. Physical security restricts physical access to information resources. It can be as simple as a locked door and as complex as money and technology will allow. [CL01, FU01, SANS06, SANS11]

E. DEFENSE IN DEPTH METHODOLOGY

The DOD leads the way in defining the Defense in Depth (DID) methodology to achieve network security in an untrusted environment. This methodology can be applied to any information system or network. The DID methodology integrates people, operations, and technology to establish multiple layers and dimensions of defense mechanisms across an information infrastructure. Multiple layers help to ensure that vulnerabilities in one layer will be covered by the other layers. Each layer and its associated technologies complement the protection provided by the other layers and

technologies. Thus, DID is essentially a combination of all of the methodologies previously discussed, in addition to lesser defense tools/concepts/implementations that are not major "methodologies", but nonetheless can contribute to the DID strategy. A key point to DID is that it employs multiple tools of the same type, such as more than one IDS; and more than one technology, such as the application of filtering in addition to an IDS. [AS01, CN01, CSRC01, FU01, HA01, NA02, NA04, NE01, NE02, SANS04, SANS07, SANS09, SY02]

There are many possible tools that can be used in a DID protection strategy. The DMZ is one tool that hasn't been previously discussed. It is the perimeter network segment that is logically between internal and external networks that is also known as a screened subnet. It provides un-trusted, external subjects with restricted access to specific applications and services. [AS01, CN01, FU01, HA01, NA02, NE01, NE02, SANS07]

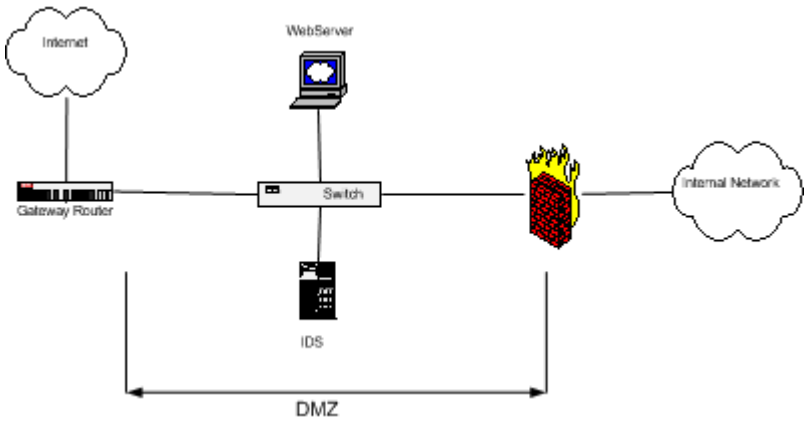

Figure 7. Illustration of DID with DMZ.

Mechanisms employed to provide DID allow one type of protection to fail without compromising the entire defensive infrastructure. This assumes the different mechanisms of defense do not share vulnerabilities. Because of the variety and number of attack methods and attackers, the DID methodology reduces the risk of successful attacks by employing many methods of defense each addressing different kinds of attacks and attackers. [AS01, FU01, HA01, NA02, NA04, NE01, SANS04, SANS07]

F. SUMMARY

Information assurance can not be accomplished by a single security mechanism or technology. The methodology that gives the greatest coverage and reduction in risk is the Defense in Depth methodology. [FU01, HA01, HA02]

Of all of the methodologies presented, none have a pre-defined directed approach to their design or implementation. All of the methodologies are ad-hoc and conducive to escalation, but none have any formal escalation process. Some of the mechanisms presented are conducive to a predefined escalation process. This process could be another dimension in the DID methodology, by incrementally increasing the defensive technologies. A predefined escalation process would enhance the ability of the DOD to attain the goals of the INFOCON system.

V. RECOMMENDATIONS

There is only one goal of the INFOCON system. It is to protect DOD systems while still supporting accomplishment of the systems' mission. A subordinate goal is to coordinate the overall defensive effort of the DOD through adherence to standards. These goals will not be realized if the system is inadequate, over reactive, or difficult to use. In support of these goals the DOD instituted the directive for the DOD Information Technology Security Certification and Accreditation Process or DITSCAP. This directive and those that implement it, require all DOD systems to be certified and have established a baseline level of IA. The existing INFOCON has no correlation or integration with the DITSCAP. [BU01, DOD03, DOD05, DOD06, RA02]

The existing INFOCON system was written by policy makers, not by technical people. The ambiguity of the criteria of each level and the reactive nature of the recommended actions are the result. The previous chapter was a detailed analysis of that system. This chapter will detail the evolution of the INFOCON system using a technical perspective. In addition to the existing INFOCON goals, the recommended system will endeavor to seamlessly integrate itself into DOD IA community procedures.

A. LEVELS

There are many things to be taken into consideration when creating a warning system. The primary consideration is for whom the warning system is being developed. Since the goal of the INFOCON system is to protect DOD systems, this warning system is designed for use by those whose jobs are to do just that.

1. Demarcation Method

The demarcation method is based on limiting the external exposure of the information infrastructure. This will be done by basing the exposure on the Mission Assurance Categories (MAC) from the DITSCAP. The MAC represents the amount of integrity and availability required for a system and has three levels. MAC III is the lowest level and it covers systems that handle day to day business, but don't materially affect support of forces in the short term. It requires only basic integrity and

availability.[13] Systems that are important to support forces are covered by MAC II, which requires high integrity and medium availability. The highest level, MAC I, covers systems that are vital to the operational readiness or mission effectiveness of the forces both in terms of content and timeliness. It requires both high integrity and high availability. [BU01, DOD03, DOD05, DOD06]

2. Number of Levels

The logical demarcation of the levels would be the primary determination of the number of levels. A secondary influence is the granularity that would provide the most efficient management. If there are too many levels the system administrators will be overwhelmed. Too few levels will result in insufficient granularity to address the threat or subsequent risk. For these reasons, the number of levels selected is four. The lowest level actually encompasses the two lowest levels of the existing INFOCON.

3. Description

The description of a level could be by color, by name, or by some well-known, pre-ordered sequence (e.g., the Greek alphabet: *Alpha*, *Beta*, *Gamma*, etc.) or any combination of these. Using names that are borrowed from an ordered sequence is naturally intuitive to remember; and the additional association of a color with each name accommodates easy visual recognition in certain environments.

For the four levels chosen there will be a descriptive name and a color. The color will allow quick, visual confirmation with other warning systems. The names are based upon limiting the exposure of the systems that accomplish the mission. These are shown in Figure 8.

[13] Please see http://www.nstissc.gov/Assets/pdf/4009.pdf (February 2004) for definitions of integrity and availability.

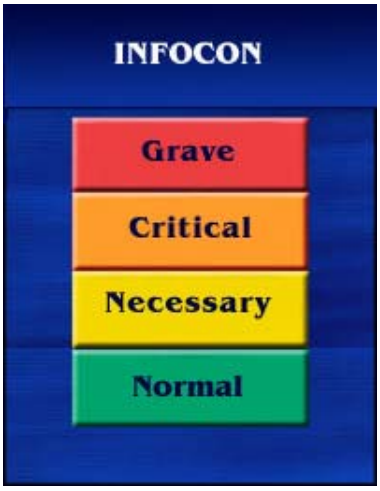

Figure 8. INFOCON Levels

All of the DOD networks are required to use the DID methodology. Therefore it is an assumption that all networks using the INFOCON will be fully hardened using the DID methodology. The Normal level represents the norm in which all systems can conduct business. The restriction of access to MAC III systems, which would be the necessary non-mission critical systems, is the Necessary level. The consequences of the loss of availability and integrity can be tolerated or overcome. The Critical level represents the restriction of access to, but not complete isolation of, MAC II systems, which are mission critical systems that are important to support forces, and the complete blockage of MAC III systems. The critical consequences of the loss of integrity are unacceptable and the loss of availability can only be tolerated for a short time. The restriction of access to MAC I systems and the complete blockage of all other systems is the Grave level. The grave consequences of the loss of integrity or availability are unacceptable. By limiting the exposure of systems in an incremental manner, each level makes the network more secure. [BU01, DOD03, DOD05, DOD06]

4. Criteria

As with the existing INFOCON system, a sufficient increase in threat level will warrant an increase to a corresponding protection level in this chapter's new recommended INFOCON level. There will be two categories of criteria in this newly proposed INFOCON system. One category will define the criteria used by the JTF-CNO to select the appropriate INFOCON level for the entire DOD.The other will be for all of

the entities under the DOD, which will be referred to from this point on as components. This separation will give DOD components a more standardized set of criteria and processes to follow. It will also allow the JTF-CNO to know how the components will respond. Both categories of criteria will be directly influenced by the SANS INFOCON, FPCON, DEFCON, WATCHCON, and CNA-WATCHCON warning systems. [SANS00]

a) JTF-CNO DOD Criteria

The JTF-CNO DOD criteria will be based upon the correlation of indicators from warning systems, reports from the commands, and the risk to the overall system. This correlation will be understandably subjective because of the nature of the stored information, the massive size and complexity of the network, and the impact to the DOD's ability to complete its mission.

By correlating the indicators from the other warning systems, it will give the JTF-CNO the ability to take into account threat indications from other arenas, such as intelligence and technical. The SANS INFOCON addresses the threats of malicious network activity and loss of connectivity, which affects the DOD just like everyone else. Correlating the FPCON addresses the terrorist threat to information systems and the Internet infrastructure. The DEFCON addresses the threats to military operations, which may require the information infrastructure to keep our war-fighters safe. The WATCHCON and the CNA-WATCHON address not only the state sponsored hacker threat, but also the rogue political group threat to the information systems.

Threat and incident reports from individual DOD components will also be correlated. These reports will indicate the overall condition of the DOD information infrastructure. Other reports contributing to the overall threat picture will contain information regarding planned and ongoing military operations; thus incorporating additional aspects pertaining to the condition and demands on the information infrastructure.

Finally, the risk to the DOD information infrastructure will be assessed. This criterion will actually be a composite of all of the other criteria and any additional information not addressed here. The risk to the information infrastructure

must be weighed against the need to accomplish the mission. This is an extremely difficult and subjective criterion, because of those concerns.

b) Component Criteria

Components will have their own sets of indicators, and their responses to these, within the general DOD framework. The component criteria will be based upon indicators from warning systems, operations planned or ongoing, technical indicators, and the risk to their systems. The operations planned or ongoing for each component will be different and thus only addressable by that component. The risk is unique to each component, because each component's information will be valued differently and their systems make up may be different. Therefore, each component will address these criteria differently.

By correlating the indicators from the other warning systems, each of the recommended INFOCON levels will have a corresponding "threat". The SANS INFOCON would map level to level, thereby addressing the threats of malicious network activity and loss of connectivity. The other warning systems each have five levels, so the first two levels of each of those systems will correspond to the lowest INFOCON level.

Mapping the FPCON levels to the INFOCON levels addresses the terrorist threat to information systems. The DEFCON represents the major military operations planned or ongoing, and so it addresses the threats to those operations, as would the WATCHCON. The CNA-WATCHON addresses not only the state sponsored hacker threat, but also the rogue political group threat to the information systems.

The technical indicators address the hacker/network threat. Some of the technical indicators will also be contained within the SANS INFOCON. Network surveillance activities (i.e., scanning and mapping) are the technical indicators for the level Normal. The technical indicators for the Necessary level are network probes or activities indicating concentrated, intrusive, reconnaissance activities (i.e., network enumeration). A network attack, whether it is successful or not, is the technical indicator for the Critical INFOCON level. The technical indicator for the Grave level is a successful network attack that attempts to gain access to trusted systems (i.e., pilfering).

5. Roles and Responsibilities

The JTF-CNO will coordinate and assess all incoming reports. It will correlate indications from the JTF-CNO DOD criteria and decide the state of the DOD information infrastructure. The JTF-CNO will be responsible for dispersing information to the components via the INFOCON level.

SAs and SSAs will be responsible for gathering technical indicators and the warning system levels. These would include the DOD INFOCON level, the SANS INFOCON level, the DOD FPCON level, the DEFCON level, and, if possible, the WATCHCON and CNA-WATCHCON levels. This information, along with the recommendation of the SA or SSA for the command's INFOCON, will be presented to the Commanding Officer.

Commanding Officers, COs, are the final authority on their command's INFOCON level. They must be able to understand the information and recommendations presented by the SAs/SSAs. The COs must correlate it with knowledge of their commands' mission, and any other information relevant to the situation. (i.e., a classified WATCHCON in effect).

B. SAFEGUARD MEASURES

The safeguard measures are in addition to sound general security practices, such as those detailed by the NSA.[14] The safeguard measures, as part of a DID implementation, will protect DOD systems and networks. It is assumed that all DOD components employ the DID methodology. Though it is still a draft, it is also assumed that the Ports, Protocols, and Services Management (PPSM) DOD instruction is being applied. The details of what ports and protocols to block for PPSM are classified. The guiding principle of denying all access except that necessary to conduct official "command" business must be followed. [DOD08]

[14] Please see http://www.issa-utah.org/pdf/sd-7.pdf (February 2004) for "The 60 Minute Network Security Guide"

Application of the least privilege principle in this manner is known as Deny by Default, and is the primary perimeter defense strategy. The perimeter is the principal method of limiting exposure and is the boundary between a component's network and all other outside networks to which it may be connected. At the Normal level this boundary has gates that are open to allow commerce and communication to flow freely. The boundary stiffens and the gates limit the traffic between the component and the Internet at the Necessary level. At the Critical level, the gates limit the traffic to only that to and from the mil domain. Since this recommended INFOCON behavior is for the DOD alone, this is a feasible strategy. All traffic be must pass the gates via an encrypted tunnel at the Grave level.

However, the component at the other end of the tunnel may not be at the same INFOCON level and therefore not be following the same policies and procedures. If that component is at a lower INFOCON level, this may expose the higher INFOCON level component. Unfortunately, if each component necessarily raised itself to the highest level of any other component it communicated with, there would be a cascade effect that, given sufficient time and communication, could eventually encompass the entire DOD. So this exposure is inescapable because it is not feasible to make the entire DOD respond to such an event.

Most of the existing INFOCON recommended actions are general policies in the DOD. These are still pertinent and can be found in Appendix F. [RA02]

The suggested safeguard measures are technical actions and are detailed in Table 1. The measures take into account that communication within the DOD must always be available. The myriad of possible network topologies and DID implementations make it impossible to create a fixed set of safeguard measures that are appropriate for in every instance. Instead, the safeguard measures elaborated upon here will be for a prototypical network and the commonly supported network services found on it. It is also assumed that existing reporting procedures will be utilized. [DOD03, DOD07, DOD08]

Area/Tools	Normal	Necessary	Critical	Grave
Perimeter				
All	Install latest patches, Updates			
Gateway Router	Deny by Default	Deny by Default; Allow port 80	Deny by Default; Allow port 80	Block all ports except VPN
	Don't allow untrusted addresses to port 53			
	Disable any unused interfaces and mgmt ports			
	Block certain ICMP (allow obd Echo)(allow inbd Echo Reply, Dest Unreachable)	Block all ICMP		
	Block inbound traceroute			
	Log each stmt blocked by filters			
	Logging is at lowest level. (Cisco=Errors) Logs sent to SysLog server.	Set logging to one level below medium. (Cisco=Warnings)	Set logging to medium level. Log all traffic. (Cisco=Notifications)	The Highest/most serious level of logging. Send logs to dedicated printer. (Cisco=Information)
	Block inbound IPs from protected network, local host, or multicast addresses			
	Block outbound IPS that have external IP as source IP, Block packets with same src/dest. IP and port.			
	Restrict access to small set of computers telnet access to internal interfaces. Log all connections.	Disallow telnet access to the router.		
	Restrict access to small set of computers SSH access only. Log all connections		Disallow external SSH access to the router	
	Sample two reliable NTP servers for time			
	Set all log messages to the same IP source address of an internal network interface			
Firewall	Deny by Default	Deny by Default;Allow port 80	Deny by Default; Allow port 80	Block all ports except VPN
	Log each stmt blocked by filters			

	Logging is at lowest level. (Cisco=Errors) Logs sent to SysLog server.	Set logging to one level below medium. (Cisco=Warnings)	Set logging to medium level. Log all traffic. (Cisco=Notifications)	The Highest/most serious level of logging. Send logs to dedicated printer. (Cisco=Information)
Mgd Switch	Deny by Default	Deny by Default; Allow port 80	Deny by Default; Allow port 80	Block all ports except VPN
	Deny Voice over IP			
	Isolate critical systems on their own vlan			Restrict access to critical vlans
	Logging is at lowest level. (Cisco=Errors) Logs sent to SysLog server.	Set logging to one level below medium. (Cisco=Warnings)	Set logging to medium level. Log all traffic. (Cisco=Notifications)	The Highest/most serious level of logging. Send logs to dedicated printer. (Cisco=Information)
	Log each stmt blocked by filters			Log all traffic to critical vlans
	Password protect all interfaces and mgmt ports			
	Sample two reliable NTP servers for time			
Detection				
All	Install latest patches, Updates			
Scanner	Externally Port Scan network 2/month	Externally Port Scan network 1/week	Externally Port Scan network daily	Externally Confirm VPN, NTP ports visible
Pwd Cracker	Run 2/month	Run weekly	Run daily	
Syslog	Disable unnecessary servers and accounts on log host.			
	Audit weekly	send Email alerts to SA; Audit 2/week	Audit logs daily	Audit logs twice a day
IDS	Monitor TCP/IP, UDP traffic from gateway rtr;	Monitor all traffic gateway rtr	Monitor all traffic firewall	
	Enable the fastest alert mode	Enable the full alert mode		
Virus Scanners	Run daily on all computers		Run 2/day	
Services				
All	Install latest patches, Updates			
	Shutdown unnecessary services			
	Each service is on a dedicated host.			

Web	Remove all unnecessary services on web server host	Block access to Internet Mail	Put up static content web site	Stop web service
	Isolate the web server physically and virtually			
	Separate content into separate directories	Make all non executable directories read only	Make all content read only, not executable	
	Enable web site logging. Audit weekly.	Audit daily		
	Audit system binaries 2/month	Audit system binaries weekly	Audit system binaries daily	
	Remove all samples installed			
FTP	Only allow if necessary for the misstion. Anonymous FTP allowed.	Require Authentication to FTP server. Disable Anonymous FTP.	Disallow writes to public directories via FTP	Stop FTP Service
SNMP	Don't use std community strings, restrict access to SNMP server	Allow read only access.	Log all access.	Disable all SNMP servers
DNS	Disable the BIND name daemon on non-DNS servers.			
	Enable logging. Audit weekly	Audit 2/week	Audit daily	
DHCP	Enable logging. Audit weekly	Audit 2/week	Audit daily	
PDC / Active Directory	Log all unsuccessful login attempts; Log every action by root account.	Log all login attempts; log attempts by unprivileged users to administrative actions		
Printers	Block all external access			
Dial in access	Authenticate using network login	Restrict access to auth numbers	Block access	
	Number isn't in the grouping of the org			
	Don't publish the number			
Applications				
All	Install latest patches, Updates			
	Enable App logging at lowest level	Enable App logging at medium level	Enable App logging at highest/most serious level	

Email	Don't open attachments unless trusted source	Encrypt all email to non .gov and .mil sites.	Allow email to and from .mil only and require digital signatures	Encrypted email to .mil only
	Block .bas, .bat, .chm, .com, .cpl, .crt, .exe, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .msi, .msp, .mst, .pif, .pl, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .ws, .wsc, .wsf, .wsh attachments	Block all Microsoft Office attachments.	Block all attachments.	
FTP	Disable unless necessary	Disable external access	Disable	
TELNET	Disable external access. Disable internal use unless necessary	Disable		
r cmds	Disable external access. Disable internal use unless necessary	Disable internal access	Disable	
SSH		External allowed to gov't & mil sites	External allowed to mil sites	Internal access only
SendMail	Don't display the version number.	Disable external access	Disable	
	Decode alias isn't available			
VPN	Available for telecommuting		Restrict external VPN access	Only access allowed through the perimeter
Backup	Complete backup weekly, incremental or differential backups in between	Complete backup twice weekly, incremental or differential backups in between	Complete backups daily	
Databases	Disable external access unless necessary		Restrict external access to critical databases	Restrict access to critical databases
Operating Systems	Enable logging. Audit weekly	Audit 2/week	Audit daily	

Table 1. Suggested INFOCON Safeguard Measures.

C. SUMMARY

The evolution of the INFOCON is based upon the analysis of the existing INFOCON, policies and goals of the DOD, and a desire to detail a system that is useful and standardized. The suggested INFOCON has four levels that are demarcated by the amount of exposure of its systems based upon the mission assurance categories of the

DITSCAP. It has two categories of criteria to determine the INFOCON level, one to be used by the JTF-CNO to determine the DOD INFOCON level and the other to be used by the DOD components. This allows standardization of the criteria for the DOD components. It also lessens the subjectivity of the decision process by giving guidance on technical threats and direct correlation of the other warning systems.

The suggested INFOCON protects the DOD information infrastructure by employing proactive and preventive actions that can incrementally increase its security posture, while still allowing for mission accomplishment. By not focusing on the potential or existing threats and instead focusing on a proactive defense-in-depth protection strategy, the suggested INFOCON attempts to lessen risk by greatly reducing the exposure of vulnerable systems. This also makes the information infrastructure more secure against both known and unknown threats.

Each area of defense has devices or services associated with it. These can be used to counter certain explicit and implicit threats for each of the suggested INFOCON levels. Some of these devices/services are good candidates for implementing predefined security escalation scripts. These candidates must also meet other considerations before they can be selected as the prototype devices/services to run the predefined security escalation scripts.

A primary consideration for such devices and services is the ability to manage that device or service from one location using a script. This would allow one SA or SSA to securely escalate the security of the entire network from one location. The use of a simple command line interface to run the escalation scripts is more secure and would not require the certification and accreditation that a GUI interface would require.

Another consideration is the security relevancy of the device or service to the security of the network. The service or device should be a key part of the security of the network.

A third consideration is the probability that the device or service is included in most DOD networks. The make, model, or version of the device or service is not part of

this consideration. Just that the general category of device or service, such as a gateway router, should be included in most DOD networks.

Two devices and a service that are likely to be in most DOD networks are a gateway router, a managed switch, and a Syslog server. Devices such as a gateway router and managed switches could have security escalation scripts written for them that could be invoked from a single/central security administrator's machine. Syslog is a service that the devices report to. The information that is sent to the Syslog server can be escalated. So the escalation for the Syslog server is the escalation in the volume/granularity of information it collects.

A gateway router is the first device or tool on a network that can filter and re-route data, so it is very relevant to the security of the network. Managed switches also filter and re-route data, but they can also isolate segments of the network, which is network security relevant. The Syslog server is the central collection point for security relevant events received from routing/switching devices, other detection tools, and various potential target services on the protected network.

Each of these mechanisms protects against different types of threats. They also meet the three considerations discussed. For these reasons, a gateway router, a managed switch and a Syslog server were selected as the prototype safeguard mechanisms.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SAFEGUARD MEASURES SCRIPTS

By focusing on a defense in depth proactive protection strategy, the suggested INFOCON protects the DOD information infrastructure by proactive and preventive techniques that enable the accomplishment of the mission. Some of the devices and tools employed in this strategy are good candidates for implementing predefined security escalation scripts. A gateway router, a managed switch, and a Syslog server were selected as the prototype devices and tool to run these escalation scripts to demonstrate these concepts.

This chapter will detail the design considerations, the structure of the scripts, the scripts themselves, and the devices and tool utilized. The network, on which the prototype scripts will be run, will be described, as well as the considerations of that network. Finally, generalizations derived from this prototype will be presented.

A. SCRIPT CONSIDERATIONS

There were several considerations used in regards to the design, development, and implementation of the escalation scripts. The first consideration was whether to manage the device scripts in a distributed manner or to centrally manage the scripts. The device scripts would be called by a single, main script that would be located on the administrator's machine.

It is easier to maintain and update scripts when they are in one location rather than spread across an entire network. However, if that location becomes compromised than all of those scripts are suspect. That may mean the perimeter has already been breached and the scripts suspect any way.[15] It is common for SAs of large networks to push changes for large number of routers using centralized scripts. So, for our example, it was determined that the scripts would be managed centrally.

The next consideration was focused on the gateway router and the managed switch. Should there be a single configuration file located on the device that contains all of access control lists (ACLs), which function as filters and self protection mechanisms,

[15] A insider would not be considered to have breached the perimeter security.

for every level of the suggested INFOCON and the script only changes the ACL for each interface? Or should there be a configuration file for each INFOCON level that the script loads into the device?

It is faster to just change the ACL for each interface, but then the configuration files must be kept on the device and in another location for documentation. Managing the configuration files in a central location doesn't require the configuration files be kept in two places, it does require that the entire configuration file be transferred to change the level on the device. Maintaining two copies of the same document presents the difficulty of keeping those documents synchronized. Nothing is more frustrating and dangerous than believing that the device is using one configuration file, when it actually has another. Thus, the configuration files and the escalation scripts should be centrally managed.

B. PROTOTYPE NETWORK

Originally, the devices and tool to be prototyped were part of an existing, suitable network in a laboratory environment. However, because of the unexpected rapid development of this network into a bastion network an alternative had to be improvised. A small network was created for the sole purpose of developing and testing the predefined escalation scripts.

This small network consists of a Cisco 2600 Router, Cisco 2590 Managed Switch, a server, a user machine, and an administrative machine. The server is both the TFTP server and the Syslog server. Unfortunately, the gateway router for this network does not support SSH...

This will require the use of telnet to manage the scripts, which is less secure because it transmits the passwords in the clear. The safeguard measures recommends the use of SSH instead of telnet for that reason. The configuration files have been modified appropriately to allow telnet in this instance. Figure 9 is the network diagram for this prototype network.

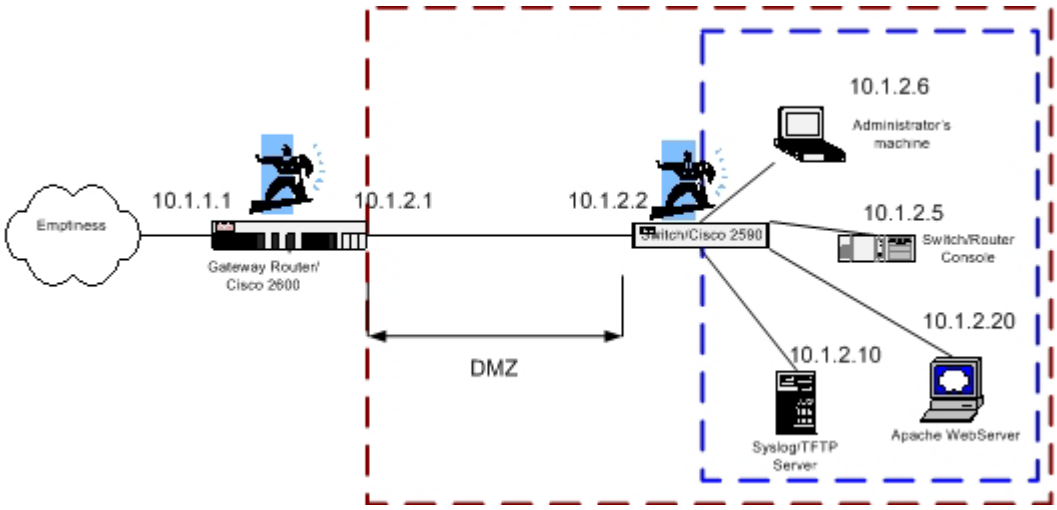

Figure 9. Prototype Network Diagram

C. SCRIPTS

Each of the mechanisms selected protect against different threats. The gateway router is the primary perimeter defense mechanism that will mitigate the threat of most amateur attackers, known as Script Kiddies. The managed switch is a second layer perimeter defense mechanism that mitigates the better Script Kiddies, the insider threat, and allows isolation of critical systems. Syslog is a detection mechanism that will help protect against the insider threat, external threats, and mitigate successful intrusions by the analysis of the events contained within its logs. [FI01, KO01, RO01, ST01]

Each mechanism's particular mitigating actions will be initiated by the command line escalation scripts. The purpose of the scripts is to allow a single SA or SSA to securely manage the security of the entire network from one location. These scripts are proof of concepts to be viewed as examples. [FI01, KO01, RO01, ST01]

There are three scripts, respectively called infocon, router, and switch. All of the scripts are located on one machine, the SA or SSA computer, and in the same directory. The main script, called infocon, was conceived so that the "push a single button concept" could be accomplished. It is the controlling script. It calls the router script and then the switch script. Figure 10 is a graphical representation of this control flow.

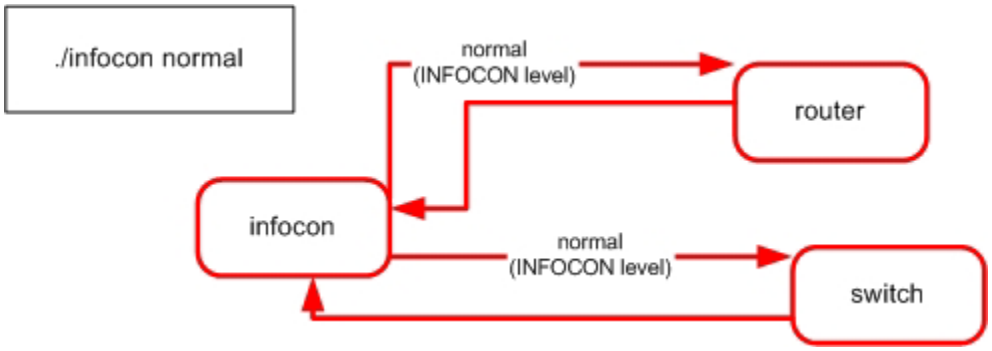

Figure 10. Flow diagram of prototype scripts

1. Infocon

This script, which is takes the INFOCON level as an argument, calls the device escalation scripts and passes the INFOCON level to the device escalation scripts. So with the command ‘./infocon grave’, the gateway router and the managed switch are escalated to the highest level of security. The script is as follows:

```
#./infocon normal
level=$1
echo $level
echo "updating router"
./router $level | telnet
#
echo " "
sleep 1
echo "updating switch"
#
./switch $level | telnet
sleep 1
#
#echo "updating webserver"
./webserver $level | telnet
sleep 1
echo "updating complete"
#end
[FI01, KO01, RO01, ST01]
```

2. Gateway Router

The managed switch was an old Cisco 2600. The particular mitigating actions to be taken by a gateway router are described in Table 1 under Gateway Router. The actual configuration files for each INFOCON level are included in Appendix H. The gateway

router script also takes the INFOCON level as an argument and is piped to telnet. The command ‘./router normal | telnet necessary’ escalates the gateway router to the second lowest level of security. Even though the configuration files are “copied” into the startup-config and the running-config files, it is not a true copy. The Cisco operating system for the router actually merges two files, when one is copied over the other. For this reason, to eliminate the Access Control Lists (ACLs) a configuration file without any ACLs, noACLs.txt, must be copied over the startup-config and the running-config files first.

The script is as follows:

```
#./router normal | telnet
#
level=$1
#
tftp=10.1.2.10
#
#
rtr=10.1.2.1
port=23
#
RtrPasswd=jennifer
#
#echo $rtr
echo open ${rtr} ${port}
sleep 1
#sleep 1
echo ${RtrPasswd}
sleep 1
#
sleep 1
echo "enable"
sleep 1
echo "thesis"
sleep 1
#
echo "copy tftp://$tftp//home/tftp/router/noACL.txt startup-config"
sleep 1
echo "startup-config"
sleep 10
#
echo "copy tftp://$tftp//home/tftp/router/$level.txt startup-config"
sleep 1
```

```
echo "startup-config"
sleep 10
#
echo "copy tftp://$tftp//home/tftp/router/noACL.txt running-config"
sleep 1
echo "running-config"
sleep 10
#
echo "copy startup-config running-config"
sleep 2
echo "running-config"
sleep 25
echo exit
#end
```

[FI01, KO01, RO01, ST01]

3. Managed Switch

The managed switch was a new Cisco Catalyst 2590. The particular mitigating actions to be taken by a managed switch are described in Table 1 under Managed Switch. This switch has the ability to use access lists to authenticate ports. Not all ports will have this ability. The actual configuration files for each INFOCON level are included in Appendix I. The managed switch script also takes the INFOCON level as an argument and is piped to telnet. The command './switch normal | telnet normal' sets the managed switch to the lowest level of security.

The script is as follows:

```
#./switch normal | telnet
#
level=$1
#
tftp=10.1.2.10
#
#
switch=10.1.2.2
port=23
#
SwPasswd=termpassword
#
echo open ${switch} ${port}
sleep 1
echo ${SwPasswd}
sleep 1
#
```

```
echo "enable"
sleep 1
echo "secret"
sleep 1
#
echo "copy tftp://$tftp//home/tftp/switch/$level.txt startup-config"
sleep 1
echo "startup-config"
sleep 10
echo "copy startup-config running-config"
sleep 2
echo "running-config"
sleep 25
echo exit
#end
[FI01, KO01, RO01, ST01]
```

4. Syslog

There are no configuration files for the Syslog server, because its purpose is to receive the logs sent to it by other network devices. It is the central repository for all event logs. By having all devices log to the same location, this makes it easier for the SA or SSA to analyze the event logs and detect a breach in the network or an insider.

D. SUMMARY

A small network consisting of a Cisco 2600 Router, Cisco 2590 Managed Switch, a TFTP server, a Syslog server, a user machine, and an administrative machine was created for the development, testing, and implementation of the predefined escalation scripts. The router does not support SSH, so the configuration files were modified appropriately.

There were two considerations in the design of the scripts that were addressed. First, the predefined escalation scripts would be managed centrally, locating them on the administrator's machine. Secondly, the configuration files would be managed centrally on the TFTP server. This allows the maximum ease of documentation and maintenance.

The predefined escalation scripts were designed, developed, tested, and successfully implemented. These scripts allow the suggested INFOCON to protect the

DOD information infrastructure by employing proactive and preventive techniques in a standardized manner. This standardization is part of the foundation that allows the DOD and its components to accomplish their mission.

The successful escalation prototype concept can be applied to other components in the network. An Apache Web server, which is an application, was included in the prototype network to demonstrate that concept. Its script is detailed in Appendix G. The script primarily alters the level of logging that the web server sends to the Syslog server.

Most applications, devices, and tools have logging capabilities. So, the safeguard measures regarding logging for the router could be applied to all applications, devices, and tools on the network. This is an example of how to apply the escalation prototype concept to other components on the network.

.

VII. CONCLUSIONS

In summary, this body of work has presented the INFOCON and the foundation of its evolution. The warning systems that influence the INFOCON were discussed. The analysis of the INFOCON followed.

This analysis answered several thesis questions. *How are the INFOCON levels defined?* The INFOCON levels are not explicitly defined. The probability of an attack and the severity of the impact of an attack are the implied methods of definition for the INFOCON levels that were selected. These definitions lead into the next question. *How are the INFOCON levels demarcated?* The method of demarcation of the INFOCON levels is the risk posed to DOD information systems. There was not a "cutoff" criterion between the layers. Nor was there a common "theme" that could be leveraged when choosing the safeguard measures to be applied.

The analysis of the network defense methodologies answered several more questions. *What is the current landscape of network defense methodologies?* It revealed that all of the methodologies were ad-hoc and conducive to escalation, but none had any formal escalation process.

Some of the mechanisms presented were conducive to a predefined escalation process. These same mechanisms could accommodate a semi-automated predefined escalation process. This would enhance the ability of the DOD to attain the goals of the INFOCON system.

The suggested INFOCON system is an information warning system whose goal is to protect DOD systems while still supporting accomplishment of the mission. Limiting the exposure of systems that support the mission is the stated method of demarcation for its four levels. Its base level, Normal, represents a fully hardened information infrastructure whose defense is based on the DID methodology and is conducting normal day to day operations. The next level, Necessary, limits the exposure of the MAC III systems and should be maintainable indefinitely. Critical, which is the third level, limits

the exposure of MAC II systems and should be maintainable for a reasonable duration. Finally, Grave limits the exposure of MAC I systems and should only be maintained for the minimum possible time.

The criteria have been separated into two categories to facilitate the standardization of determining the INFOCON level. The direct correlation of other warning systems to each INFOCON level and the technical indicators at the component level are the two criteria that are not subjective. All of the criteria for the JTF-CNO are subjective due to the size, complexity, and nature of the DOD information infrastructure.

The suggested INFOCON protects the DOD information infrastructure by proactive techniques that enable the accomplishment of the mission. By focusing on a strong proactive defense in depth strategy, the suggested INFOCON incrementally lessens the exposure of the systems thereby making the information infrastructure more secure against known and future threats. This answers the question; *What is the appropriate tactical response to each of the INFOCON levels?*

The ability to secure the information infrastructure against known and future threats is one of the suggested INFOCON system's greatest benefits. It also offers the users of the system a system designed from their perspective, thus allowing greater user acceptance and understanding, which are both key to the success of any warning system. The suggested safeguard measures are specific, technical, and feasible, which removes ambiguity and replaces it standardization.

In Table 1, each area of defense has devices associated with it that mitigate implied or expected threats for each of the suggested INFOCON levels. Some of the devices mentioned in the safeguard measures are good candidates for implementing predefined security escalation scripts. Thus, another thesis question could be answered: *What security-implementing devices would make good candidates for implementing the security scripts?* Devices such as the gateway router, the managed switch, and a Syslog server are good candidates to receive escalation scripts that could be run from one machine. These devices were selected as the prototype devices.

Can the safeguard scripts be centrally managed? This was a question that needed to be answered before the design and development of the predefined escalation scripts. It is less complicated and faster to push changes for a large number of network components using centralized scripts. So, it was determined that the configuration files and the escalation scripts could be centrally managed.

The suggested INFOCON is quite feasible technically, as demonstrated by the simplicity of the prototype scripts. The existing INFOCON system is currently being re-engineered by the JTF-CNO and the suggested INFOCON system could be an option for the JTF-CNO to consider. It is a fresh perspective on the warning system at the very least.

A. CONCLUSIONS

The goal of the INFOCON system is to protect DOD systems while still supporting accomplishment of the mission. The suggested INFOCON system accomplishes that goal because it is based upon supporting the mission. It also accomplishes the goal of coordinating the overall defensive effort of the DOD through adherence to criteria and demarcation standards provided by the Mission Assurance Categories.

B. FUTURE WORK

There are several areas for future work, research, and development. Here are just a few:

- Working with the JTF-CNO to develop the next INFOCON system.
- In depth analytical assessment of the relationship among the numerous warning systems.
- Analysis and development of reporting procedure to better integrate the existing warning systems.
- Development of real-time automated log auditing.

- Development of a sound technique of auditing logs to reveal insider threats.
- Feasibility study of integrating the INFOCON into the DITSCAP.
- Formal mathematical analysis (Ph.D. level research) of the demarcation of the INFOCON levels.
- Development of an efficient event reporting procedure between JTF-CNO and the DOD components in regards to the INFOCON.

APPENDIX A – ACRONYMS

ACL……..Access Control List

ARPANET…Advanced Research Projects Agency Network

CJCS…….Chairman of the Joint Chiefs of Staff

CNA……..Computer Network Attack

CNA WATCHCON…. Computer Network Attack Watch Condition

COTS……Commercial off the Shelf

DEFCON…. Defense Readiness Condition

DID……Defense in Depth

DII…….DOD information infrastructure

DITSCAP….DOD Information Technology Security Certification & Accreditation Process

DOD……..Department of Defense

DoS……...Denial of Service

EMP……..Electromagnetic pulse

FPCON……Force Protection Condition

GAO……General Accounting Office

HSAS……...Homeland Security Advisory System

I&W…….Indications and Warning

IDS……...Intrusion Detection System

INFOCON...Information Operations Condition

IA…….Information Assurance

IP……. Internet Protocol

IPsec……Internet Protocol Security

IS…….Information System

JTF-CND…Joint Task Force, Computer Network Defense

JTF-CNO…Joint Task Force, Computer Network Operations(formerly JTF-CND)

QoSS……...Quality of Security Service

PPSM……...Ports, Protocols, and Service Management

SA……System Administrator

SecDef……..Secretary of Defense

SSA……..System Security Administrator

SSH……..Secure Shell

TCP……..Transmission Control Protocol

THREATCON…Terrorist Threat Condition

WATCHCON….Watch Condition

APPENDIX B – TERMS AND CONCEPTS

Accreditation — It is the authorization granted by the designated approving authority that permits a DOD system to process, store, and/or transmit information. It is based upon information gathered during the certification process and concerns the protection and defense of the information and/or the system. [BU01]

Availability — The concept of information assurance that guarantees that the information or service is accessible (available) when it is sought.

Certification — The comprehensive evaluation of the technical and non-technical security features of a system and other safeguards to establish the extent to which a particular design and implementation meets a set of specified security requirements. [BU01]

Information Assurance — "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation." [DOD03]

Integrity — The concept of information assurance that assures that there is no unauthorized modification or deletion of data.

Internet Protocol — A set of rules designed for use in interconnected systems of packet switched computer communication networks. [IN02]

Internet Protocol Address — A numerical address, expressed in the format specified in the Internet Protocol, for devices and resources. [FU01]

IP Address — See "Internet Protocol Address".

IPsec — A tunneling protocol used primarily by VPNs.

Transmission Control Protocol — A set of rules that works in conjunction with IP that defines how data is sent in the form of message units between computers over a packet switched computer communication networks. IP handles the actual delivery of the data. TCP tracks the individual units of data, which is called a packet, that a message is divided into for efficient routing through the packet switched computer communication network. [FU01]

Virtual Private Network (VPN) — A virtual private network that is a secure communications channel for data networking incorporating IPsec.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C – INFOCON ENCLOSURE (SOURCE RA02)

1. Purpose. The Information Operations Condition (INFOCON) recommends actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to the DOD information infrastructure, including computer and telecommunications networks and systems. The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system impacts all personnel who use DOD information systems, protects systems while supporting mission accomplishment, and coordinates the overall defensive effort through adherence to standards.

2. Description. The INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on DOD computer and telecommunication networks and systems. While all communications systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and standoff capability make computer network attack (CNA) an attractive option to our adversaries at present. The DOD INFOCON criteria and response actions may be expanded at a later date to include all forms of information operations. CNA is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity; unauthorized access; and data browsing. DOD INFOCON measures focus on computer network-based protective measures, due to the unique nature of CNA (reference paragraph 5). Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are NORMAL (normal activity), ALPHA (increased risk of attack), BRAVO (specific risk of attack), CHARLIE (limited attack), and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions.

3. Authority. The INFOCON system is established by the Secretary of Defense, and administered through the Director for Operations, Joint Staff (J-3). The INFOCON system will be administered through the Commander, Joint Task Force for Computer Network Defense (JTF-CND), when the JTF-CND reaches initial operational capability (IOC). All combatant commands, Services, directors of Defense and combat support agencies will develop supplemental INFOCON procedures as required, specific to their command and in consonance with this guidance. Subordinate and operational unit commanders will use the INFOCON procedures developed by their higher headquarters (e.g., combatant commands or Services). Existing policy and procedures on communications security (COMSEC) may be integrated into local INFOCON procedures at the commander's discretion.

4. Applicability. This document provides guidance for standardized procedures and sets responsibilities for authorizing and communicating INFOCONs as part of information operations (IO) throughout the Department of Defense. The information contained herein applies to the Joint Staff; Services; combatant commands; Defense agencies; and joint, combined, and other DOD activities throughout the entire conflict spectrum -- peacetime through war.

5. Assumptions. Several critical assumptions were made about the nature of computer network attack (CNA) in developing the DOD INFOCON system. Understanding these assumptions is essential to effectively implement this system.

a. Shared Risk. In today's network-centric environment, risk assumed by one is risk shared by all. Unlike most other military operations, a successful network intrusion in one area of responsibility (AOR) may, in many cases, facilitate access into other AORs. This necessitates a common understanding of the situation and responses associated with the declared DOD INFOCON. These actions must be carried out concurrently in all AORs for an effective defense.

b. Advance Preparation. Preparation is key, given the speed and reduced signature of CNA. Protective measures must be planned, prepared, exercised, and often executed well in advance of an attack. Preventive measures are emphasized in INFOCON responses because there may be little time to react effectively during the attack. Prevention of system compromise (see Appendix C for various advisories to consider) is preferable, but may not be achievable.

c. Anonymity of Attacker. Attributing the attack to its ultimate source, if possible, will normally not occur until after the attack has been executed. This limits the range and type of options available to military decision makers. To effectively operate in this environment, knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics.

d. Characterization of the Attack. Distinguishing between hacks, attacks, system anomalies, and operator error may be difficult. The most prudent approach is to assume malicious intent until an event is assessed otherwise. (See Appendix C for various assessments to consider.)

6. Structure. This paragraph explains the INFOCON structure, including level, brief description, criteria to declare, and recommended actions. The criteria listed are broad guidance for the commander to consider when declaring an INFOCON, not concrete thresholds. All criteria for a particular INFOCON need not be met to change to that level. More detailed explanation of routine security measures such as internal security reviews and external vulnerability assessments are located in Appendix A, General Security Practices.

LABEL	CRITERIA	RECOMMENDED ACTIONS
NORMAL **Normal Activity**	No significant activity.	• Ensure all mission critical information and information systems (including applications and databases) and their operational importance are identified. • Ensure all points of access and their operational necessity are identified. • On a continuing basis, conduct normal security practices. For example: • Conduct education and training for users, administrators, and management. • Ensure an effective password management program is in place. • Conduct periodic internal security reviews and external vulnerability assessments. • Conduct normal auditing, review, and file back-up procedures. • Confirm the existence of newly identified vulnerabilities and install patches. • Employ normal reporting procedures IAW para 7d. • Periodically review and test higher level INFOCON actions.
ALPHA **Increased Risk of Attack**	• Indications and warning (I&W) indicate general threat. • Regional events occurring which affect U.S. interests and involve potential adversaries with suspected or known CNA capability. • Military operation, contingency or exercise planned or ongoing requiring increased security of information systems. • Information system probes, scans or other activities detected indicating a pattern of surveillance.	• Accomplish all actions required at INFOCON normal. • Execute appropriate security practices (see Appendix A). For example: • Increase level of auditing, review, and critical file back-up procedures. • Conduct internal security review on all critical systems. • Heighten awareness of all information system users and administrators. • Execute appropriate defensive tactics. • Employ normal reporting procedures IAW para 7d. • Review and test higher level INFOCON actions, and consider proactive execution.
BRAVO **Specific Risk of Attack**	• I&W indicate targeting of specific system, location, unit or operation. • Major military operation or contingency, planned or ongoing. • Significant level of network probes, scans or activities detected	• Accomplish all actions required at INFOCON ALPHA. • Execute appropriate security practices (see Appendix A). For example: • Increase level of auditing, review, and critical file back-up procedures. • Conduct immediate internal security review on all critical systems. • Confirm existence of newly identified vulnerabilities and install patches. • Disconnect unclassified dial-up connections not required

	indicating a pattern of concentrated reconnaissance. • Network penetration or denial of service attempted with no impact to DOD operations.	for current operation. • Execute appropriate defensive tactics. • Ensure increased reporting requirements are met IAW para 7d. • Review and test higher level INFOCON actions, and consider proactive execution.
CHARLIE **Limited Attack(s)**	• Intelligence attack assessment(s) indicate a limited attack. • Information system attack(s) detected with limited impact to DOD operations: • Minimal success, successfully counteracted. • Little or no data or systems compromised. • Unit able to accomplish mission.	• Accomplish all actions required at INFOCON BRAVO. • Execute appropriate response actions. For example: • Conduct maximum level of auditing, review and critical file back-up procedures. • Consider minimize on appropriate computer networks and telecommunications systems (limit traffic to mission essential communication only). (Ssee Appendix E, ref. e, CJCSI 6900.01A) • Reconfigure information systems to minimize access points and increase security. • Reroute mission-critical communications through unaffected systems. • Disconnect non-mission essential -critical networks • Employ alternative modes of communication and disseminate new contact information. • Execute appropriate defensive tactics. • Ensure increased reporting requirements are met IAW para 7d. • Review and test higher level INFOCON actions, and consider proactive execution.
DELTA **General Attack(s)**	• Successful information system attack(s) detected which impact DOD operations. • Widespread incidents that undermine ability to function effectively. • Significant risk of mission failure.	• Accomplish all actions required at INFOCON CHARLIE. • Ensure increased reporting requirements are met IAW para 7d. • Execute applicable portions of continuity of operations plan (Ssee Appendix E, ref. f, DODD 3020.26, Ccontinuity of Ooperations, Ppolicy and Pplanning). • Designate alternate information systems and disseminate new communication procedures internally and externally. • Execute procedures for ensuring graceful degradation of information systems. • Implement procedures for conducting operations in "stand-alone" mode or manually. • Isolate compromised systems from rest of network. • Execute appropriate defensive tactics.

7. Procedures

a. Determining the INFOCON. There are three broad categories of factors that influence the INFOCON: operational, technical, and intelligence, including foreign intelligence and law enforcement intelligence. Some factors may fall into more than one category. The INFOCON level is based on significant changes in one or more of them. Appendix C describes several factors that may be considered when determining the INFOCON. DOD organizations are frequently confronted with unauthorized access to

information systems. The decision to change the INFOCON should be tempered by the overall operational and security context at that time. For example, an intruder could gain unauthorized access and not cause damage to systems or data. This may only warrant INFOCON ALPHA or NORMAL during peacetime, but may warrant INFOCON CHARLIE during a crisis; or it may warrant a high INFOCON at the affected unit, but not throughout the command or the Department of Defense as a whole.

b. Declaring INFOCONs. The Joint Staff J3/Commander, JTF-CND (CJTF) will recommend changes in DOD INFOCON through the CJCS to the SecDef IAW paragraph 3. Assimilation and evaluation of information to assess the CND situation DOD-wide will be a collaborative effort focused at the Joint Staff/JTF-CND. The Secretary of Defense may delegate declaration authority to the J-3/CJTF. Commanders are responsible for assessing the situation and establishing the proper INFOCON based on evaluation of all relevant factors. Commanders may change the INFOCON of their organizations; however, they must remain at least as high as the current INFOCON directed by SecDef or the Chairman of the Joint Chiefs of Staff. The commander will report changes in INFOCON IAW subparagraph 7d.

c. Response Measures. Response measures associated with INFOCONs are normally recommended actions unless specifically directed by SecDef. Ideally, CND operations will be based on advanced warning of an attack. The intelligence community is developing a capability to provide warning which will become of increasing value as it matures. Measures should be commensurate with the risk, the adversary's assessed capability and intent, and mission requirements. Over-aggressive countermeasures may result in self-inflicted degradation of system performance and communication ability, which may contribute to the adversary's objectives. Commanders must also consider the impact imposing a higher INFOCON for their command will have on connectivity with computer networks and systems of other commands. Combatant commands will notify the Joint Staff if recommended or directed response measures conflict with theater priorities. Additionally, response measures directed by combatant commands will take precedence over response measures directed by Service INFOCONs when applicable. Regardless of the INFOCON level declared at the affected site, it is incumbent upon the affected site to report all unauthorized accesses in a timely manner IAW subparagraph 7d.

d. Reporting. Technical reporting will be accomplished IAW reference A. Report violations of the law (such as unauthorized access to military computer networks and systems) to servicing military counterintelligence organizations IAW DODI 5240.6, "Counterintelligence Awareness and Briefing Program," and with local and Service/command policy. However, INFOCONs assess potential and/or actual impact to DOD operations and must be reported through operational channels. Additional guidance on INFOCON reporting follows.

(1) Reporting Channels. Combatant commands, Services, and DOD agencies will report INFOCON changes and summary reports to the Joint Staff through the National Military Command Center (NMCC):

CJCS NMCC WASHINGTON DC//J3/J33/J39//

Combatant commands, Services, and DOD agencies will designate a reporting authority and establish reporting procedures for organizational entities under their jurisdictions. Service entities under the operational control of a combatant command will follow the reporting instructions of that combatant command. Individual Service policy may require information copies to higher Service headquarters. Those entities not reporting directly to a CINC will follow Service-reporting procedures (usually to the Service operations center, which would then forward the information to the NMCC).

(2) Reporting Frequency. Services, combatant commands, and Defense agencies will report INFOCON changes to the NMCC NLT 4 hours after the INFOCON has changed. Provide whatever information is available at the time and indicate fields that are unknown or unavailable. Report information missing from the initial report in a follow-up report when it becomes available. Services, combatant commands, and Defense agencies may dictate more frequent internal reporting to subordinate components.

(3) Report Formats. Reports of changes in INFOCON should be accompanied by an operational assessment of the situation when appropriate. Appendix D outlines a process for assessing the operational impact of a computer network attack. Reports will include, as a minimum:

(a) For all INFOCONs: unit/organization and location, date/time of report, current INFOCON, reason for declaration of this INFOCON, response actions taken, POC (name, rank, duty title, contact information).

(b) INFOCON BRAVO and higher. All of the above, plus: unit/organization mission, current operation(s) (name, type, and AOR) unit is supporting, upcoming operation(s) (name, type, AOR, and dates) unit is projected to support, Service computer emergency/incident response team (CERT/CIRT) or DISA Automated Systems Security Incident Support Team (ASSIST) incident number and law enforcement agency (LEA) case number with POC contact information.

(c) INFOCON CHARLIE and higher. All of the above, plus: system(s) affected (network, classification, application, database/data file), degree to which operational functions are affected (command and control; intelligence, surveillance and reconnaissance; movement/maneuver; sustainment; fires; and protection), impact (actual and/or potential) on current/planned missions and/or general capabilities, restoration priorities, workarounds.

(4) Dissemination of DOD INFOCON. The Joint Staff/JTF-CND will send notification to combatant commands, Services, and agencies when the DOD INFOCON is changed. Commands, Services, and agencies are responsible for notifying units assigned to them. Notification will include the following information:

(a) Date/time of report.
(b) Current INFOCON.
(c) Reason for declaration of this INFOCON.
(d) Current/planned operation(s) or capabilities, units/organizations, networks, systems, applications or data assessed to be impacted or at risk.
(e) Recommended or SecDef-directed actions.
(f) References to relevant technical advisories, intelligence assessments, etc.
(g) POC contact information.

8. Security. Classification guidance and disclosure policy concerning IO is addressed in reference c. Specific guidance related to INFOCON follows.

a. INFOCON labels and descriptions are unclassified.

b. Generic defensive measures, when not tied to a specific INFOCON, are unclassified. Specific measures may be published in a classified appendix, if required.

c. Measures to be taken by all personnel, regardless of INFOCON, are unclassified.

d. General criteria to declare an INFOCON are FOR OFFICIAL USE ONLY (FOUO). Specific criteria may be published in a classified appendix, if required.

e. Classification of the measures associated with a particular INFOCON is the responsibility of the originator and will be classified according to content. However, the measures associated with a particular INFOCON, in aggregate, may require a higher classification than the individual measures. The measures associated with a particular INFOCON, in aggregate, will be FOUO at a minimum.

f. The operational impact of a successful information attack is classified SECRET or higher.

g. CNA intelligence assessments are classified SECRET or higher.

h. Information associated with an ongoing criminal investigation of a CNA may be considered law-enforcement sensitive.

i. A combatant command, Service, or agency may authorize release of its INFOCON system and procedures to allies or coalition partners as necessary to ensure effective protection of its information systems. Locally developed INFOCON procedures

should use DODI 3600.2 and the guidance above when considering release to allies or coalition partners.

j. Changes in INFOCON are operational security (OPSEC) indicators and must be protected accordingly. The criteria and response measures are also of value to foreign intelligence Services in assessing the effectiveness of a CNA and in analyzing DOD's response. Do not post INFOCON procedures in publicly accessible locations such as unit web pages on unclassified networks and bulletin boards accessible to outsiders.

9. Relationship of INFOCON to Other Alert Systems. The INFOCON, THREATCON, DEFCON, CNA-WATCHCON, and conventional WATCHCON all interact with each other when the situation warrants it. The INFOCON may be changed based on the world situation (THREATCON, DEFCON), the intelligence community's level of concern (CNA-WATCHCON, conventional WATCHCON), or other factors (reference Appendix C). Likewise, a change in INFOCON may prompt a corresponding change in other alert systems.

a. The defense condition (DEFCON) is a uniform system of progressive conditions describing the types of actions required to bring a command's readiness to the level required by the situation (reference d).

b. The threat condition (THREATCON) is a process that sets the level for a terrorist threat condition at a given location, based on existing intelligence and other information.

c. A watch condition (WATCHCON) is part of the defense warning system indicating the degree of intelligence concern with a particular warning problem.

d. A CNA-WATCHCON is an intelligence assessment that takes into account CNA threat levels, as well as the overall political situation (reference b).

e. The INFOCON addresses risk of attack and protective measures for information and information systems.

10. Assessment

a. Exercises. INFOCON procedures should be practiced in all joint and/or combatant command exercises.

b. Combatant commands, Services, and agencies are requested to submit feedback to the Joint Staff on the effectiveness of the INFOCON system based on real-world and exercise data. The Joint Staff will review the system periodically to ensure it satisfies operational requirements.

11. These procedures are effective immediately and will remain in effect until superseded by DOD instruction.

12. List of Appendixes

a. General Security Practices.
b. Defensive Tactics.
c. Factors Influencing the INFOCON. See Annex A to Appendix C: CNA Intelligence Assessment Sample Format.
d. Operational Impact Assessment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A - GENERAL SECURITY PRACTICES

Listed below are several measures that can significantly reduce the risk of successful attack against a critical information system. These activities should be the foundation of a sound, prevention-based information assurance/security program.

a. System Security Administration. All DOD activities must ensure their systems are administered by technically qualified, experienced personnel who are provided periodic professional training in system administration and security, as well as the necessary tools to assist in effective baseline management, auditing, and network intrusion detection. Configuration management, proper staffing, and strong systems policies are critical to reliable and secure operations.

b. Auditing/Log Review. All DOD activities should regularly review audit logs for suspicious activity, IAW Appendix E, reference a and locally existing guidance. Logging and review requirements may increase with increases in INFOCON, including more frequent reviews, focused string searches, analysis of activity below normal trigger thresholds, and submission of logs to an organization designated to conduct specialized reviews.

c. Critical File Back-up Procedures. All DOD activities should conduct periodic back-ups of files critical to mission accomplishment, IAW Appendix E, reference a and locally existing guidance. Storage of back-up files should be isolated from any network and physically separated from the originating facility. Increases in INFOCON may warrant changes in the frequency of back-ups from quarterly, monthly, or weekly to daily or real-time.

d. Internal Security Reviews. All DOD activities should establish procedures for conducting internal security reviews, IAW reference a and locally existing guidance. These reviews should consist of, as a minimum, the following actions:

(1) Check password strengths (searching for default and weak passwords).
(2) Review pertinent technical advisories; install patches, implement fixes, execute preventive/mitigating actions.
(3) Conduct information system vulnerability scans.
(4) Identify network access points and their operational importance.
(5) Raise awareness level of all users as new vulnerabilities are found.
(6) Examine historically dormant/infrequently used accounts for signs of unusual activity.

e. External Vulnerability Assessments. All DOD activities should establish procedures for coordinating with outside agencies (e.g., Service CERTs/CIRTs, DISA, and NSA) to conduct vulnerability assessments and analyses of their information systems, IAW existing guidance. These assessments may include network scans, OPSEC surveys, COMSEC reviews, and red team operations.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B - DEFENSIVE TACTICS

1. The following list of defensive tactics offers possible responses to several types of suspicious/unauthorized activity. Defensive tactics should not be executed without some knowledge of the degree to which an intruder has penetrated the system and careful consideration of the potential, practical and legal consequences. For instance, changing passwords to lock out unauthorized access to valid accounts may not be prudent if a sniffer has been installed which can capture the new passwords.

2. Types of Activity. Adversary activity may be categorized as reconnaissance/suspicious activity, unauthorized access, denial of service, data browsing, data corruption, and malicious code. Conducting activities such as data browsing and data corruption is dependent upon gaining access to the system. Therefore, actions that prevent or halt unauthorized access might also be used to counteract data browsing and corruption.

3. General Actions. The following actions may or may not be valid responses to several or all types of malicious activity. The decision whether or not to employ them depends on the severity of the attack, and the practical and legal issues relating to such actions.

a. Disseminate reports/alert messages with suspicious Internet Protocol (IP) addresses, attack profiles/signatures.

b. Review thresholds for defensive systems (e.g., firewalls) and update for new/detected threats.

c. Freeze/eliminate compromised or unauthorized accounts.

d. Isolate affected network segment.

e. Re-route intruder to dummy network.

f. Jam communication lines.

g. Review thresholds for defensive systems and update for new/detected threats.

h. Tag critical files.

i. Block offending IP addresses/telephone lines.

j. Isolate compromised portions of affected system and monitor/log all activity.

k. Re-route intruder to a decoy system and continue logging activity.

l. Refer to identified technical advisories/alerts (Service CERTs/CIRTs, DISA ASSIST, NSA IPC, etc.).

m. Recall key information system security personnel.

n. Activate crisis action team to respond to impact of adversary CNA.

4. Reconnaissance/Suspicious Activity

a. Description. Automated scans/manual probes of networks to ascertain if the target system has known vulnerabilities or to get general information about the target system.

b. Possible defensive actions include reconstructing the scan/probing to determine what information was revealed, monitoring all incoming activity from the source IP address, blocking all access from the source IP address.

5. Denial of Service

a. Description: any action that causes all or part of the affected network's service to be stopped entirely, interrupted, or degraded sufficiently to impact network operations. Service may be denied by crashing the system, jamming it with packets, or consuming disk space, processor time or other resources.

b. Possible defensive actions include blocking all incoming activity from the source IP address/phone line.

6. Unauthorized Access

a. Description. Entry into and use of a system by an unauthorized individual.

b. Possible defensive actions include changing passwords; blocking all access from the source IP address; freezing/eliminating compromised, infrequently used, or historically dormant user accounts.

7. Data Browsing

a. Description. Unauthorized reading, capturing and/or downloading of information stored on or transmitted over a network.

b. Possible defensive actions for stored information include: encrypt files/directories; generate dummy files to confuse browsers; hide and/or rename key files

or directories; transfer sensitive files from servers to auxiliary storage media; tag potential target files.

c. Possible defensive actions for transmitted information include point-to-point encryption, flooding transmission lines with useless information, employing COMSEC procedures (limit traffic, use codes), using cover accounts.

8. Data Corruption

a. Description. Unauthorized modification of the contents of a file, database, or transmission. Ranges from subtle alterations that may not be noticed to complete destruction of the information, rendering the file, database, or transmission unusable.

b. Possible defensive actions include resetting file/directory access controls; backing up key verifiable files onto CD-ROM; using back-up files; storing key files/databases on removable storage media; employing checksums, signature files, and file tagging; developing a counter-deception plan.

9. Malicious Logic

a. Description. Hardware, software, or firmware intentionally inserted into an information system for an unauthorized purpose (e.g., Virus and Trojan horse).

b. Possible defensive actions include updating virus signature files and running appropriate virus detection/eradication software (if virus is known); checking all systems and signature files for unauthorized files or changes to files; removing user-specific, nonstandard applications; removing intranet web pages containing executable code fragments; disabling user-installed documents/templates containing macros.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C - FACTORS INFLUENCING THE INFOCON

When determining the appropriate defensive posture, many factors must be considered. This appendix lists several factors that commanders should consider when determining the INFOCON. (Note: This list is offered as broad guidance; other factors may be considered also.)

a. CNA-WATCHCON and threat warning assessments (reference b). Paragraph 9 and reference b provide more information on CNA-WATCHCONs. Also, other threat-warning assessments may be considered when determining the INFOCON.

b. Other indications & warning (including domestic threats). NSA IPC Alerts; National Infrastructure Protection Center (NIPC) advisories, threats, warnings; Service law enforcement agency intrusion reports, etc.

c. CNA intelligence assessment. (See Annex A for sample format). This report provides a fused intelligence assessment of the attack. US intelligence organizations work within legal restrictions on collecting and retaining information on US persons, IAW Executive Order 12333 and implementing DOD and Service regulations. Intelligence personnel will ensure mission accomplishment and compliance with relevant intelligence law by coordinating closely with law enforcement personnel. In the event that a CNA assessment leads intelligence personnel to US person information which they are legally prevented from pursuing further, they will transfer the matter to appropriate law enforcement organization, who will then produce a similar CNA assessment report, sanitized to protect law enforcement-sensitive information.

d. Conventional WATCHCON. Conventional warnings on actors with CNA capability may suggest an increased risk of CNA from those actors.

e. Current world situation. Increased tensions with a nation possessing CNA capability may precede CNA operations against us.

f. Other alert systems such as DEFCON, THREATCON, etc. Reference d, paragraph 9, and local security procedures discuss various alert systems. Local commanders must determine if a change in one alert status will cause a corresponding change in another alert status.

g. Current/planned military operations. The operational context within which an event occurs is critical to determining the appropriate level of response. Any contingencies, crisis actions, exercises, or other operations a unit is supporting or projected to support must be considered when determining the INFOCON.

h. Dependence of military functions upon particular information systems. Applications directly supporting military functions (i.e., command and control; intelligence, surveillance, and reconnaissance; movement and maneuver; fires; and

sustainment) may be predominantly resident on a single network or system. For example, the Global Transportation Network (GTN) is an NIPRNET-based application. If NIPRNET is the affected system, GTN and consequently the sustainment function may be adversely impacted. This type of analysis may suggest the degree to which a particular network, system, application or database is mission critical.

i. Commander's assessment of mission-critical information system readiness. Conceptually similar to 'status of resources and training system' (sorts). Commanders may base unit ability to accomplish the mission in part on the readiness of unit computer networks and systems. This readiness may be determined from the networks' security posture, vulnerability, extent of compromise, etc.

j. Information Assurance Vulnerability Alert (IAVA) bulletins. See reference a for format and explanation.

k. Incident reports. These are roughly analogous to tactical warning/attack assessment. See reference a for format and explanation.

l. Trend analyses. Reports showing number, type, and frequency of attacks; systems targeted; hot IP addresses, etc. See reference a for format and explanation.

m. Technical impact assessment. This information may be included in an incident report, or may result from follow-on analysis. This assessment may include the extent of system compromise and/or disruption and the degree to which system confidentiality, integrity, availability, authentication, and non-repudiation have been affected. See reference a for an explanation of these terms.

n. Operational impact assessment--a key element in determining the INFOCON. (See Appendix D for procedures.) The process for assessing operational impact also lays the groundwork for executing preventive measures, developing workarounds, and establishing restoration priorities.

o. Commander's assessment of the potential for an information attack. Although much objective data is available on which to base the decision, the final judgment for declaring an INFOCON change rests with the commander. Objective assessment of the situation and prudent analysis of all available information must be integrated with the commander's experience and leadership to determine the organization's appropriate defensive posture.

ANNEX A TO APPENDIX C
CNA INTELLIGENCE ASSESSMENT SAMPLE FORMAT

1. Reference. CNA incident source reports (include originating agency, message DTG).

2. Executive Summary. Between 1 and 4 sentences summarizing significant elements of report.

3. Incident Summary. The following information is available from incident reports (reference a) and is included as background in this section of the intelligence assessment report:

a. Time and duration of incident.
b. CNA technique employed.
c. Path of attack/identification and location of origin of attack.
d. Location of system/network targeted.
e. Unit subordination of system/network targeted.
f. Mission of system/network targeted.
g. Actual impact of attack.
h. Potential impact of attack.

4. Intelligence Assessment. Consistent with intelligence law restrictions on the collection of US person information, the following information will be generated by intelligence analysts and included in this section of the intelligence assessment report:

a. Assessed source of attack. (Who did it? A certain terrorist group, government, or sub-organization defined to the best extent possible.)

b. Assessed type of attack. (What did they do? How? Provide simple explanation of the technical basis of the attack technique or tools from the perspective of insights into adversary capabilities.)

c. Assessed motivation of attack. (Why did they do it? Collect intelligence, implant malicious logic, harass/distract, disrupt operations, etc.)

d. Supporting analysis for both of the above assessments. (In addition to the logical inferences based on the current situation, background data should be provided—known CNA organizations, past practices, doctrine, etc.)

e. Contextual data on the situation. (What else is going on other than CNA that is potentially relevant to the current situation?)

f. Follow-on projection. (What can we expect next from the perpetrator? What about use of the particular CNA technique by others?)

APPENDIX D - OPERATIONAL IMPACT ASSESSMENT

1. Assessing the impact of CNA on our ability to conduct military operations is key to conducting damage assessment, prioritizing response actions, and assisting in identifying possible adversaries. This appendix offers an operational impact assessment process that may be used when reporting changes in INFOCON. Note: assessment results are classified SECRET at a minimum. The assessment process itself is unclassified.

2. Prior to an attack:

a. Identify all critical information systems.

b. For each critical information system, identify all resident critical applications and databases.

c. Determine which military functions are supported by each application/database: command and control; intelligence, surveillance, and reconnaissance; movement and maneuver; fires; sustainment; and protection.

3. After an attack or attempted attack has been detected:

a. Identify all critical information systems targeted.

b. List operations the unit is currently supporting or projected to support in the near future.

c. For each information system targeted, determine the technical impact, i.e., to what degree are confidentiality, integrity, availability, authentication, and non-repudiation affected? What critical applications and databases are impacted?

d. For the technical impacts identified, estimate the time and resources required to restore functionality. Identify any interim workarounds.

e. How does the technical impact of the attack affect the unit's ability to function?

f. How does the impact to the unit's ability to function affect support to current/projected operations? If no specific operations are ongoing or projected, how is general capability/readiness affected?

APPENDIX E - REFERENCES

a. CJCSI 6510.01b, Defensive Information Operations Implementation

b. DIA message 021727z JUN 98, Indications and Warning for Information Warfare/Information Operations {CNA-WATCHCON}

c. DODI 3600.2, Classification Guidance for Information Operations

d. CJCSM 3402.01A, Alert System of the Chairman of the Joint Chiefs of Staff

e. CJCSI 6900.01A, Telecommunications Economy and Discipline

f. DODD 3020.26, Continuity of Operations, Policies and Planning

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D – FPCON (SOURCE JO01)

The terrorist force protection conditions, FPCONs, outlined below describe the progressive level of a terrorist threat to all US military facilities and personnel under DOD Directive O-2000.12. As approved by the Chairman of the Joint Chiefs of Staff, the terminology and definitions are recommended security measures designed to ease inter-Service coordination and support of US military antiterrorism activities. The purpose of the FPCON system is accessibility to, and easy dissemination of, appropriate information. The DOD Directive O-2000.12 recommended measures are:

- **FPCON NORMAL** exists when a general threat of possible terrorist activity exists but warrants only a routine security posture.
- **FPCON ALPHA** applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCONs resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.
    - Measure 1. At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of US installations. Watch for abandoned parcels or suitcases and any unusual activity.
    - Measure 2. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.
    - Measure 3. Secure buildings, rooms, and storage areas not in regular use.
    - Measure 4. Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.
    - Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.
    - Measure 6. As a deterrent, apply measures 14, 15, 17, or 18 from FPCON BRAVO either individually or in combination with each other.
    - Measure 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher THREATCONs.
    - Measure 8. Review and implement security measures for high-risk personnel as appropriate.
    - Measure 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.
- **FPCON BRAVO** applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for

weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

- Measure 11. Repeat measure 1 and warn personnel of any other potential form of terrorist attack.
- Measure 12. Keep all personnel involved in implementing antiterrorist contingency plans on call.
- Measure 13. Check plans for implementation of the next FPCON.
- Measure 14. Move cars and objects (e.g., crates, trash containers) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.
- Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.
- Measure 16. At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.
- Measure 17. Examine mail (above the regular examination process) for letter or parcel bombs.
- Measure 18. Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.
- Measure 19. Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense, and to build confidence among staff and dependents.
- Measure 20. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.
- Measure 21. At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.
- Measure 22. Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Identify the visitor's destination. Ensure that proper dignity is maintained, and if possible, ensure that female visitors are inspected only by a female qualified to conduct physical inspections.
- Measure 23. Operate random patrols to check vehicles, people, and buildings.
- Measure 24. Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or exiting the vehicle.
- Measure 25. Implement additional security measures for high-risk personnel as appropriate.
- Measure 26. Brief personnel who may augment guard forces on the use of deadly force. Ensure that there is no misunderstanding of these instructions.
- Measures 27. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

- **FPCON CHARLIE** applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this FPCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

- Measure 30. Continue, or introduce, all measures listed in FPCON BRAVO.
- Measure 31. Keep all personnel responsible for implementing antiterrorist plans at their places of duty.
- Measure 32. Limit access points to the absolute minimum.
- Measure 33. Strictly enforce control of entry. Randomly search vehicles.
- Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.
- Measure 35. Issue weapons to guards. Local orders should include specific orders on issue of ammunition.
- Measure 36. Increase patrolling of the installation.
- Measure 37. Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.
- Measure 38. Erect barriers and obstacles to control traffic flow.
- Measure 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.

- **FPCON DELTA** applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this FPCON is declared as a localized condition.
    - Measure 41. Continue, or introduce, all measures listed for FPCONs BRAVO and CHARLIE.
    - Measure 42. Augment guards as necessary.
    - Measure 43. Identify all vehicles within operational or mission-support areas.
    - Measure 44. Search all vehicles and their contents before allowing entrance to the installation.
    - Measure 45. Control access and implement positive identification of all personnel--no exceptions.
    - Measure 46. Search all suitcases, briefcases, packages; etc., brought into the installation.
    - Measure 47. Control access to all areas under the jurisdiction of the United States.
    - Measure 48. Make frequent checks of the exterior of buildings and of parking areas.
    - Measure 49. Minimize all administrative journeys and visits.

Measure 50. Coordinate the possible closing of public and military roads and facilities with local authorities.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E – HOMELAND SECURITY PRESIDENTIAL DIRECTIVE - 3 (SOURCE WH01)

Homeland Security Presidential Directive-3

Purpose

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. Such a system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

Homeland Security Advisory System

The Homeland Security Advisory System shall be binding on the executive branch and suggested, although voluntary, to other levels of government and the private sector. There are five Threat Conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

Low = Green;
Guarded = Blue;
Elevated = Yellow;
High = Orange;
Severe = Red.

The higher the Threat Condition, the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat Conditions shall be assigned by the Attorney General in consultation with the Assistant to the President for Homeland Security. Except in exigent circumstances, the Attorney General shall seek the views of the appropriate Homeland Security Principals or their subordinates, and other parties as appropriate, on the Threat Condition to be assigned. Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted.

For facilities, personnel, and operations inside the territorial United States, all Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system and henceforth administer their systems consistent with the determination of the Attorney General with regard to the Threat Condition in effect.

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement Protective Measures rests with the Federal departments and agencies. It is recognized that departments and agencies may have several preplanned sets of responses to a particular Threat Condition to facilitate a rapid, appropriate, and tailored response. Department and agency heads are respon-sible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. Likewise, they retain the authority to respond, as necessary, to risks, threats, incidents, or events at facilities within the specific jurisdiction of their department or agency, and, as authorized by law, to direct agencies and industries to implement their own Protective Measures. They shall continue to be responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. Governors, mayors, and the leaders of other organizations are encouraged to conduct a similar review of their organizations= Protective Measures.

The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis by the Attorney General in consultation with the Assistant to the President for Homeland Security. Every effort shall be made to share as much information regarding the threat as possible, consistent with the safety of the Nation. The Attorney General shall ensure, consistent with the safety of the Nation, that State and local government officials and law enforcement authorities are provided the most relevant and timely information. The Attorney General shall be responsible for identifying any other information developed in the threat assessment process that would be useful to State and local officials and others and conveying it to them as permitted consistent with the constraints of classification. The Attorney General shall establish a process and a system for conveying relevant information to Federal, State, and local government officials, law enforcement authorities, and the private sector expeditiously.

The Director of Central Intelligence and the Attorney General shall ensure that a continuous and timely flow of integrated threat assessments and reports is provided to the President, the Vice President, Assistant to the President and Chief of Staff, the Assistant to the President for Homeland Security, and the Assistant to the President for National Security Affairs. Whenever possible and practicable, these integrated threat assessments and reports shall be reviewed and commented upon by the wider interagency community.

A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

1. To what degree is the threat information credible?
2. To what degree is the threat information corroborated?
3. To what degree is the threat specific and/or imminent?
4. How grave are the potential consequences of the threat?

Threat Conditions and Associated Protective Measures

The world has changed since September 11, 2001. We remain a Nation at risk to terrorist attacks and will remain at risk for the foreseeable future. At all Threat Conditions, we must remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are some suggested Protective Measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific Protective Measures:

1. **Low Condition (Green)**. This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:
    1. Refining and exercising as appropriate preplanned Protective Measures;
    2. Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
    3. Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
2. **Guarded Condition (Blue)**. This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
    1. Checking communications with designated emergency response or command locations;
    2. Reviewing and updating emergency response procedures; and
    3. Providing the public with any information that would strengthen its ability to act appropriately.
3. **Elevated Condition (Yellow)**. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement:
    1. Increasing surveillance of critical locations;
    2. Coordinating emergency plans as appropriate with nearby jurisdictions;
    3. Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
    4. Implementing, as appropriate, contingency and emergency response plans.
4. **High Condition (Orange)**. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
    1. Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
    2. Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
    3. Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
    4. Restricting threatened facility access to essential personnel only.
5. **Severe Condition (Red)**. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective

Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

1. Increasing or redirecting personnel to address critical emergency needs;
2. Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
3. Monitoring, redirecting, or constraining transportation systems; and
4. Closing public and government facilities.

Comment and Review Periods

The Attorney General, in consultation and coordination with the Assistant to the President for Homeland Security, shall, for 45 days from the date of this directive, seek the views of government officials at all levels and of public interest groups and the private sector on the proposed Homeland Security Advisory System.

One hundred thirty-five days from the date of this directive the Attorney General, after consultation and coordination with the Assistant to the President for Homeland Security, and having considered the views received during the comment period, shall recommend to the President in writing proposed refinements to the Homeland Security Advisory System.

APPENDIX F – INFOCON POLICY RECOMMENDED ACTIONS

Normal

- Identify all mission critical information and information systems (including applications and databases) and their operational importance.
- Identify all points of access and their operational necessity.
- Conduct periodic internal security reviews.
- Ensure an effective password management program is in place.
- Conduct education and training for users, administrators, and management.
- Heighten awareness of all information system users and administrators.
- Confirm the existence of newly identified vulnerabilities and install patches.
- Conduct internal security review on all critical systems.
- Review and test higher level INFOCON measures.
- Consider proactive execution of higher INFOCON measures.

Necessary

- Conduct immediate internal security review on all critical systems.
- Confirm existence of newly identified vulnerabilities and install patches.
- Review and test higher level INFOCON measures.
- Consider proactive execution of higher INFOCON measures.

Critical

- Employ alternative modes of communication and disseminate new contact information.
- Review and test higher level INFOCON measures.
- Consider proactive execution of higher INFOCON measures.

Grave

- Execute applicable portions of continuity of operations plan
- Disseminate new communication procedures internally and externally.
- Execute procedures for ensuring graceful degradation of information systems.
- Implement procedures for conducting operations in “stand-alone” mode or manually.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G – APACHE WEB SERVER SCRIPT

```
#./webserver normal | telnet
level=$1
#
tftp=10.1.2.10
#
webserver=10.1.2.20
port=23
#
pwd=password
#
echo open ${webserver} ${port}
sleep 1
echo "root"
sleep 1
echo ${pwd}
sleep 1
#
echo "cd .."
sleep 2
#
echo "./usr/local/sbin/apachectl stop"
sleep 3
#
echo "tftp 10.1.2.10"
sleep 1
echo "mode binary"
sleep 1
#
#get [host1:]file1 [host2:]file2 ... [hostN:]fileN
#
echo "get /home/tftp/webserver/$level.conf /usr/local/etc/apache/httpd.conf"
#
sleep 2
#
echo quit
sleep 2
#
echo "./usr/local/sbin/apachectl start"
sleep 5
echo exit
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H – GATEWAY ROUTER CONFIGURATION FILES (SOURCE CI01, FI01, KO01, NA05, RO01, ST01)

noACL.txt

```
!Disable following servers
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no service finger
no ip http server
!
!Disable following services
no cdp run
no service config
no ip source-route
no ip subnet-zero
!
!Configure the console and the virtual terminal lines () to time out a session
!Require a password at login and to allow only telnet traffic.
line con 0
exec-timeout 5 0
login
transport input telnet
line aux 0
no exec
exec-timeout 0 5
no login
transport input none
line vty 0 4
exec-timeout 5 0
login
transport input telnet
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 thesis
!
!Configure passwords for the console, aux, and the virtual terminal lines.
!Use a different password for each line.
line con 0
password jennifer
line aux 0
password jennifer
line vty 0 4
password jennifer
```

```
!
!Provide protection for above passwords by the following global config cmd.
service password-encryption
!
!Clear out a previous acl
no access-list 100
no access-list 102
no access-list 105
!
interface e0
description outer
!
interface Ethernet1
description inner
ip address 10.1.2.1 255.255.255.0
!
line vty 0 4
!
!Enable the router's logging capability
logging on
!
!Syslog level to be sent to the router console
logging console errors
!
!disable logging to all terminal lines except for the router console.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap errors
!
!set all log messages with the same IP source address of a router interface.
logging source-interface e1
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

Normal.txt

```
!Based on NSA 60min Security Guide
!
!Disable following servers
```

```
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no service finger
no ip http server
!
!Disable following services
no cdp run
no service config
no ip source-route
no ip subnet-zero
!
!Configure the console and the virtual terminal lines () to time out a session
!Require a password at login and to allow only telnet traffic.
line con 0
exec-timeout 5 0
login
transport input telnet
line aux 0
no exec
exec-timeout 0 5
no login
transport input none
line vty 0 4
exec-timeout 5 0
login
transport input telnet
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 thesis
!
!Configure passwords for the console, aux, and the virtual terminal lines.
!Use a different password for each line.
line con 0
password jennifer
line aux 0
password jennifer
line vty 0 4
password jennifer
!
!Provide protection for above passwords by the following global config cmd.
service password-encryption
!
!Clear out a previous acl
no access-list 100
```

```
no access-list 102
no access-list 105
access-list 100 permit ip 10.1.1.0 0.0.0.255 any
access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!Protect the router against the TCP SYN Attack.
!denies anyone from any external network from starting any TCP connection
access-list 100 permit tcp any 10.1.2.0 0.0.0.255 established
!
access-list 100 permit tcp any 10.1.2.0 0.0.0.255
!
access-list 100 permit ip any 10.1.2.0 0.0.0.255
!
!Allow inbound to the protected network (e.g.,10.1.2.0) only
!ICMP message types: Echo Reply, Destination Unreachable
access-list 100 permit icmp any 10.1.2.0 0.0.0.255 echo-reply
access-list 100 permit icmp any 10.1.2.0 0.0.0.255 unreachable
!
!Allow only trusted addresses to port 53
access-list 100 permit tcp host 10.1.2.6 host 0.0.0.0 eq 53 log
access-list 100 permit udp host 10.1.2.6 host 0.0.0.0 eq 53 log
!
!Provide IP address spoof protection for inbound traffic to protected network (e.g.
10.1.2.0).
!access-list 100 deny ip 10.1.2.0 0.0.0.255 any log
!access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
!
!Block inbound traceroute from a Unix computer
access-list 100 deny udp any any range 33434 33534 log
!
!Force the router to log the src and dest ports for denied TCP and UDP traffic.
access-list 100 deny udp any range 0 65535 any range 0 65535 log
access-list 100 deny tcp any range 0 65535 any range 0 65535 log
!
access-list 100 deny icmp any any log
access-list 100 deny ip any any log
!
interface e0
description outer
ip access-group 100 in
!
```

```
!Set logging on an extended IP access-list statement
access-list 102 permit tcp 10.1.2.0 0.0.0.255 any eq 80
access-list 102 permit tcp 10.1.2.0 0.0.0.255 any
!
!Provide IP address spoof protection for outbound traffic from protected network (e.g. 10.1.2.0).
access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!allow outbound from the protected network (e.g.,10.1.2.0) only
!ICMP message types: Echo
access-list 102 permit icmp 10.1.2.0 0.0.0.255 any echo
access-list 102 deny icmp any any log
access-list 102 deny ip any any log
!
interface Ethernet1
description inner
ip address 10.1.2.1 255.255.255.0
ip access-group 102 in
!
!Allow Telnet access from certain computers on the protected network (e.g., 14.4.4.0) to the router
!via an extended IP access-list. The administrator can telnet to any interface IP address on the
!router.
access-list 105 permit tcp 10.1.2.0 0.0.0.255 any eq 23 log
access-list 105 deny ip any any log
line vty 0 4
access-class 105 in
!
!Enable the router's logging capability
logging on
!
!Syslog level to be sent to the router console
logging console errors
!
!disable logging to all terminal lines except for the router console.
!no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap errors
!
!how to set time information for the logging and debugging.
```

```
!ntp server 10.1.2.10
!ntp server 10.1.2.10
!ntp source Ethernet0/1
!service timestamps log datetime localtime show-timezone
!service timestamps debug datetime localtime show-timezone
!clock timezone EST –5
!clock summer-time EDT recurring
!
!set all log messages with the same IP source address of a router interface.
logging source-interface e1
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

Necessary.txt

```
!Based on NSA 60min Security Guide
!
!Disable following servers
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no service finger
no ip http server
!
!Disable following services
no cdp run
no service config
no ip source-route
no ip subnet-zero
!
!Configure the console and the virtual terminal lines () to time out a session
!Require a password at login and to allow only telnet traffic.
line con 0
exec-timeout 5 0
login
transport input telnet
line aux 0
no exec
exec-timeout 0 5
no login
transport input none
line vty 0 4
exec-timeout 5 0
```

```
login
transport input telnet
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 thesis
!
!Configure passwords for the console, aux, and the virtual terminal lines.
!Use a different password for each line.
line con 0
password jennifer
line aux 0
password jennifer
line vty 0 4
password jennifer
!
!Provide protection for above passwords by the following global config cmd.
service password-encryption
!
!Clear out a previous acl
no access-list 100
no access-list 102
no access-list 105
access-list 100 permit ip 10.1.1.0 0.0.0.255 any
access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!Protect the router against the TCP SYN Attack.
!denies anyone from any external network from starting any TCP connection
access-list 100 permit tcp any 10.1.2.0 0.0.0.255 established
!
access-list 100 permit tcp any 10.1.2.0 0.0.0.255
!
access-list 100 permit ip any 10.1.2.0 0.0.0.255
!
!Allow only trusted addresses to port 53
access-list 100 permit tcp host 10.1.2.6 host 0.0.0.0 eq 53 log
access-list 100 permit udp host 10.1.2.6 host 0.0.0.0 eq 53 log
!
!Block all inbound icmp
access-list 100 deny icmp any any log
!access-list 100 deny ip any any log
!
!Block inbound traceroute from a Unix computer
access-list 100 deny udp any any range 33434 33534 log
!
interface e0
```

```
description outer
ip access-group 100 in
!
!Set logging on an extended IP access-list statement
access-list 102 permit tcp 10.1.2.0 0.0.0.255 any eq 80
access-list 102 permit tcp 10.1.2.0 0.0.0.255 any
!
!Provide IP address spoof protection for outbound traffic from protected network (e.g.,10.1.2.0).
access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!Block all outbound icmp
access-list 102 deny icmp any any log
!access-list 102 deny ip any any log
!
interface Ethernet1
description inner
ip address 10.1.2.1 255.255.255.0
ip access-group 102 in
!
!Allow Telnet access from certain computers on the protected network (e.g., 14.4.4.0) to the router
!via an extended IP access-list. The administrator can telnet to any interface IP address on the
!router.
access-list 105 permit tcp 10.1.2.0 0.0.0.255 any eq 23 log
access-list 105 deny ip any any log
line vty 0 4
access-class 105 in
!
!Enable the router's logging capability
logging on
!
!Syslog level to be sent to the router console
logging console warnings
!
!disable logging to all terminal lines except for the router console.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap warnings
!
```

```
!set all log messages with the same IP source address of a router interface.
logging source-interface e1
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

Critical.txt

```
!Based on NSA 60min Security Guide
!
!Disable following servers
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no service finger
no ip http server
!
!Disable following services
no cdp run
no service config
no ip source-route
no ip subnet-zero
!
!Configure the console and the virtual terminal lines () to time out a session
!Require a password at login and to allow only telnet traffic.
line con 0
exec-timeout 5 0
login
transport input telnet
line aux 0
no exec
exec-timeout 0 5
no login
transport input none
line vty 0 4
exec-timeout 5 0
login
transport input telnet
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 thesis
!
!Configure passwords for the console, aux, and the virtual terminal lines.
!Use a different password for each line.
```

```
line con 0
password jennifer
line aux 0
password jennifer
line vty 0 4
password jennifer
!
!Provide protection for above passwords by the following global config cmd.
service password-encryption
!
!Clear out a previous acl
no access-list 100
no access-list 102
no access-list 105
access-list 100 permit ip 10.1.1.0 0.0.0.255 any
access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!
!Protect the router against the TCP SYN Attack.
!denies anyone from any external network from starting any TCP connection
access-list 100 permit tcp any 10.1.2.0 0.0.0.255 established
!
access-list 100 permit tcp any 10.1.2.0 0.0.0.255
!
access-list 100 permit ip any 10.1.2.0 0.0.0.255
!
!
!Allow only trusted addresses to port 53
access-list 100 permit tcp host 10.1.2.6 host 0.0.0.0 eq 53 log
access-list 100 permit udp host 10.1.2.6 host 0.0.0.0 eq 53 log
!
!Block all inbound icmp
access-list 100 deny icmp any any log
!
access-list 100 deny ip any any log
!
!Block inbound traceroute from a Unix computer
access-list 100 deny udp any any range 33434 33534 log
!
interface e0
description outer
ip access-group 100 in
!
!Set logging on an extended IP access-list statement
access-list 102 permit tcp 10.1.2.0 0.0.0.255 any eq 80
```

```
!
!Provide IP address spoof protection for outbound traffic from protected network (e.g.,10.1.2.0).
access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!Block all outbound icmp
access-list 102 deny icmp any any log
!
!access-list 102 deny ip any any log
!
interface Ethernet1
description inner
ip address 10.1.2.1 255.255.255.0
ip access-group 102 in
!
!Allow Telnet access from certain computers on the protected network (e.g., 14.4.4.0) to the router
!via an extended IP access-list. The administrator can telnet to any interface IP address on the
!router. However, the router converts any interface IP address to 0.0.0.0.
!Thus, the unusual destination IP address 0.0.0.0 must be used in the access-list.
access-list 105 permit tcp 10.1.2.0 0.0.0.255 any eq 23 log
access-list 105 deny ip any any log
line vty 0 4
access-class 105 in
!
!Enable the router's logging capability
logging on
!
!Syslog level to be sent to the router console
logging console Notifications
!
!disable logging to all terminal lines except for the router console.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap Notifications
!
!set all log messages with the same IP source address of a router interface.
logging source-interface e1
!
!Set the syslog facility type in which log messages are sent
```

```
logging facility local7
!
end
```

Grave.txt

```
!Based on NSA 60min Security Guide
!
!Disable following servers
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no service finger
no ip http server
!
!Disable following services
no cdp run
no service config
no ip source-route
no ip subnet-zero
!
!Configure the console and the virtual terminal lines () to time out a session
!Require a password at login and to allow only telnet traffic.
line con 0
exec-timeout 5 0
login
transport input telnet
line aux 0
no exec
exec-timeout 0 5
no login
transport input none
line vty 0 4
exec-timeout 5 0
login
transport input telnet
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 thesis
!
!Configure passwords for the console, aux, and the virtual terminal lines.
!Use a different password for each line.
line con 0
password jennifer
line aux 0
password jennifer
```

```
line vty 0 4
password jennifer
!
!Provide protection for above passwords by the following global config cmd.
service password-encryption
!
!Clear out a previous acl
no access-list 100
no access-list 102
no access-list 105
access-list 100 permit ip 10.1.1.0 0.0.0.255 any
access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!Permit only VPN port, which is port 336
access-list 100 permit tcp any any eq 336
!
!Protect the router against the TCP SYN Attack.
!denies anyone from any external network from starting any TCP connection
access-list 100 permit tcp any 10.1.2.0 0.0.0.255 established
!
!Block all inbound icmp
access-list 100 deny icmp any any log
!
access-list 100 deny ip any any log
!
!Block inbound traceroute from a Unix computer
access-list 100 deny udp any any range 33434 33534 log
!
interface e0
description outer
ip access-group 100 in
!
!Set logging on an extended IP access-list statement
!access-list 102 permit tcp 10.1.2.0 0.0.0.255 any eq 80
!
!Provide IP address spoof protection for outbound traffic from protected network
(e.g.,10.1.2.0).
!access-list 102 permit ip 10.1.2.0 0.0.0.255 any
!
!Block all outbound icmp
access-list 102 deny icmp any any log
!
access-list 102 deny ip any any log
!
interface Ethernet1
```

```
description inner
ip address 10.1.2.1 255.255.255.0
ip access-group 102 in
!
!Allow Telnet access from certain computers on the protected network (e.g., 14.4.4.0) to the router
!via an extended IP access-list. The administrator can telnet to any interface IP address on the
!router. However, the router converts any interface IP address to 0.0.0.0.
!Thus, the unusual destination IP address 0.0.0.0 must be used in the access-list.
access-list 105 permit tcp 10.1.2.0 0.0.0.255 any eq 23 log
access-list 105 deny ip any any log
line vty 0 4
access-class 105 in
!
!Enable the router's logging capability
logging on
!
!Syslog level to be sent to the router console
logging console informational
!
!disable logging to all terminal lines except for the router console.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap debugging
!
!set all log messages with the same IP source address of a router interface.
logging source-interface e1
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

APPENDIX I – MANAGED SWITCH CONFIGURATION FILES (SOURCE CI01, FI01, KO01, NA05, RO01, ST01)

Normal.txt

```
hostname switch
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 jennifer
enable password jennifer
!
!need to clean out prior config file
no access-list 1
!
cdp timer 200
cdp holdtime 160
cdp advertise-v2
cdp run
!
!specify machines to manage switch
access-list 1 permit 10.1.2.0 0.255.255.255
access-list 1 deny any
line vty 0 4
access-class 1 in
!
!disable unnecessary services
no ip http server
no service pad
!
!interface
interface Vlan1
no shutdown
ip address 10.1.2.2 255.255.255.0
!
!Enable the switch's logging capability
logging on
!
!Syslog level to be sent to the switchconsole
logging console errors
!
!disable logging to all terminal lines except for the switchconsole.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
```

```
!
!Set the syslog level to be sent to the log host
logging trap errors
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

Necessary.txt

```
hostname switch
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 jennifer
enable password jennifer
!
!need to clean out prior config file
no access-list 1
!
no cdp timer
no cdp holdtime
no cdp run
!
!specify machines to manage switch
access-list 1 permit 10.1.2.0 0.0.0.255 log
access-list 1 deny any any log
line vty 0 4
access-class 1 in
!
!disable unnecessary services
no ip http server
no service pad
!
!set gateway MAC statically
!mac-addres-table static <gateway MAC> vlan 1 interface fa0/1
!
!set static ARP entry
!arp <gateway IP> <gateway MAC>
!
!interface
interface Vlan1
no shutdown
ip address 10.1.2.2 255.255.255.0
!
!Enable the switch's logging capability
```

```
logging on
!
!Syslog level to be sent to the switchconsole
logging console warnings
!
!disable logging to all terminal lines except for the switchconsole.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap warnings
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

Critical.txt

```
hostname switch
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 jennifer
enable password jennifer
!
!need to clean out prior config file
no access-list 1
!
no cdp timer
no cdp holdtime
no cdp run
!
!specify machines to manage switch
access-list 1 permit 10.1.2.0 0.0.0.255 log
access-list 1 deny any any log
line vty 0 4
access-class 1 in
!
!disable unnecessary services
no ip http server
no service pad
!
!interface
interface Vlan1
```

```
no shutdown
ip address 10.1.2.2 255.255.255.0
!
!Enable the switch's logging capability
logging on
!
!Syslog level to be sent to the switchconsole
logging console Notifications
!
!disable logging to all terminal lines except for the switchconsole.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap Notifications
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

Grave.txt

```
hostname switch
!
!Configure the Enable Secret password, protected by a MD5-based algorithm.
enable secret 0 jennifer
enable password jennifer
!
!need to clean out prior config file
no access-list 1
!
no cdp timer
no cdp holdtime
no cdp run
!
!specify machines to manage switch
access-list 1 permit 10.1.2.0 0.0.0.255 log
access-list 1 deny any any log
line vty 0 4
access-class 1 in
!
!disable unnecessary services
no ip http server
```

```
no service pad
!
!interface
interface Vlan1
no shutdown
ip address 10.1.2.2 255.255.255.0
!
!Enable the switch's logging capability
logging on
!
!Syslog level to be sent to the switchconsole
logging console informational
!
!disable logging to all terminal lines except for the switchconsole.
no logging monitor
!
!Set the IP address of the log host
logging 10.1.2.10
!
!Set the syslog level to be sent to the log host
logging trap Informational
!
!Set the syslog facility type in which log messages are sent
logging facility local7
!
end
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[AD01] http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/toc.htm October 2003.

[AN01] http://www.angelfire.com/ca7/Security/threatcon.html January 2004.

[AS01] Ashley, Bradley. Jackson, Gary. Information Assurance through Defense in Depth. Retrieved January 27, 2004. from http://iac.dtic.mil/iatac/IAnewsletter/Vol3_No2.pdf

[AU01] http://www.au.af.mil/au/awc/awcgate/awc/jenkins.pdf January 2004.

ARDA. Computer Network Defense Strategy and Tactics for the Intelligence Community. Version 7, March 2003.

[BU01] Burke, Karen. CS 4680: Certification and Accreditation. Naval Postgraduate School.

[CI01] http://www.cisco.com February 2004.

[CI02] http://cisr.nps.navy.mil/ January 2004.

[CL01] Clark, Paul. CS 3670: Secure Management of Systems. Naval Postgraduate School.

[CN01] CNSS Instruction No. 4009. National Information Assurance Glossary. Revised May 2003 found at http://www.nstissc.gov/Assets/pdf/4009.pdf

[CO01] Committee to Review DOD C4I Plans and Programs, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council. Realizing the Potential of C4I: Fundamental Challenges. NATIONAL ACADEMY PRESS Washington, D.C. 1999. Retrieved December 2003 from http://www.nap.edu/html/C4I/ch3_b3.html

[CO02] Computer Security Institute. 2003 CSI/FBI Computer Crime and Security Survey. Eighth Annual. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf January 2004.

[CSRC01] http://csrc.nist.gov/publications/nistbul/06-00.pdf January 2004.

[CSRC02] http://csrc.nist.gov/publications/nistbul/11-99.pdf January 2004.

[CSRC03] http://csrc.nist.gov/publications/nistbul/b-10-03.pdf January 2004.

[CSRC04] http://csrc.nist.gov/publications/nistbul/bulletin10-02.pdf January 2004.

[CSRC05] http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf January 2004.

[CSRC06] http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf January 2004.

[CY01] http://cybercoyote.org/security/multi-layer.htm January 2004.

[DA01] Davis, Don. Compliance Defects in Public Key Cryptography. March 10, 1997.

[DE02] Defense Science Board. *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)*, Office of the Under Secretary of Defense for Acquisition and Technology. Washington, D.C. 1996.

[DE03] http://www.developer.com/tech/article.php/641471 January 2004.

[DI01] DIA message 021727Z JUN 98, Indications and Warning for Information Warfare/Information Operations (CNA-WATCHCON).

[DI02] Dinolt, George W. CS 4605: Security Policies and Models and Formal Methods. Naval Postgraduate School.

[DI03] http://www.disa.mil, December 2003.

[DOD01] DOD Directive O-2000.12, "DOD Antiterrorism (AT) Program" November 21, 2003.

[DOD02] DOD Directive S-3600.1, "Information Operations (IO) (U)," December 6, 1996.

[DOD03] DOD Directive 8500.1 "Information Assurance (IA)" Certified Current as of November 21, 2003. Retrieved February 5, 2004 from http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf

[DOD04] DOD Handbook 2000.12-H, "Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February 19, 1993.

[DOD05] DOD Instruction 5200.40, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)", 30 December 1997. Retrieved December 2003 from http://iase.disa.mil/ditscap/DitscapFrame.html

[DOD06] DOD Instruction 8500.2 "Information Assurance (IA) Implementation" February 6, 2003. Retrieved February 6, 2004 from http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf

[DOD07] DOD Instruction 8550.bb "Ports, Protocols and Services Management (PPSM)", 20 March 2003.

[DOD08] DOD "Draft 021030 Incorporating revised Risk Category Definitions and Assignments: NIPRNET Ports, Protocols, Services (PPS) Security Technical Guidance" Release 1 Retrieved February 11, 2004 from https://infosec.navy.mil/pub/docs/documents/dod/dodd/niprnet_port_protocol_guide_draft.doc

[DT01] http://www.dtic.mil/doctrine/jel/doddict/data/p/03997.html January 2004.

[DT02] http://www.dtic.mil/whs/directives/corres/pdf/d200012_081803/d200012p.pdf#xml=http://www.dtic.mil/search97/s97is.vts?action=View&VdkVgwKey=http%3A%2F%2Fwww%2Edtic%2Emil%2Fwhs%2Fdirectives%2Fcorres%2Fpdf%2Fd200012%5F081803%2Fd200012p%2Epdf&doctype=xml&Collection=whs&QueryZip=FPCON& November 2003.

[EM01] http://emd.wa.gov/6-rr/e-ops/nat-thrt/ntws/1 January 2004.

[EU01]http://www.eucom.mil/Directorates/ECPA/News/index.htm?http://www.eucom.mil/directorates/ecpa/news/FPCON.htm&2 January 2004.

[FA01]http://www.fas.org/irp/doddir/dod/app-J_THREATCON.htm January 2004.

[FA02]http://www.fas.org/nuke/guide/usa/c3i/defcon.htm January 2004.

[FI01] Fiedler, D. & Hunter, B. (1988). *UNIX System Administration.* Indianapolis: Hayden

[FU01] Fulp, J.D. CS 3690: Network Security. Naval Postgraduate School.

[FU02] Fulp, J.D. Research Idea for ARDA Challenge. Naval Postgraduate School Memorandum, July 2003.

[FU03]http://www.funet.fi/index/FUNET/history/internet/en/arpanet.html November 2003.

[GL01] http://www.globalsecurity.org/military/ops/oplan-5027-2.htm November 2003.

[GM01] http://cne.gmu.edu/modules/acmpkp/security/history_frm.html October 2003.

[GO01] http://www.gocsi.com/press/20030528.jhtml January 2004.

[HA01] Harkins, Richard. CS 3600: Information Assurance: Introduction to Computer Security. Naval Postgraduate School.

[HA02] Hazlewood, Victor. Defense in Depth: Information Assurance for 2003. Retrieved January 2, 2004 from http://www.sdsc.edu/~victor/publications/DefenseInDepthWhitePaper.doc

[HT01] http://httpd.apache.org/docs-2.0/programs/httpd.html March 2004.

[IE01] http://www.ieas.or.kr/vol11_4/yoontaeyoung.htm October 2003.

[IN01] INFORMATION ASSURANCE Legal, Regulatory, Policy and Organizational Considerations. 4th Edition. August 1999. http://www.dtic.mil/jcs/j6/j6k/ia.pdf October 2003.

[IN02] Information Sciences Institute of the University of Southern California. RFC: 791 Internet Protocol – DARPA Internet Program Protocol Specification. Dated September 1981.

[IR01] Irvine, Cynthia E. CS 4600: Secure Systems. Naval Postgraduate School.

[JO01] Joint Tactics, Techniques, and Procedures for Antiterrorism, APPENDIX J THREATCON SYSTEM. Joint Pub 3-07.2 17 March 1998.

[KE01] Kellogg, Jospeh. http://armedservices.house.gov/openingstatementsandpressreleases/107thcongress/01-05-17kellogg.html October 2003.

[KE02] http://www.koreaembassyusa.org/bilateral/military/eng_military3.cfm November 2003.

[KO01] Kochan, S. & Wood, P. (1988). *UNIX Shell Programming.* Indianapolis: Hayden

[LU01] http://www.luke.af.mil/pubs/lukeafbpubs/LAFBI33-206.doc November 2003.

[MC01] McClure, Stuart. Scambray, Joel. Kurtz, George. Hacking Exposed, Network Security Secrets & Solutions. 4th Edition. February, 2003

[NA01] http://www.nae.edu/nae/naehome.nsf/weblinks/CGOZ-58NLKV?OpenDocument January 2004.

[NA02] http://www.nap.edu/books/0309064856/html/141.html January 2004.

[NA03] http://www.nap.edu/html/C4I/ch3_b3.html January 2004.

National Computer Security Center. Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria. Rainbow Series. 31 July 1987.

[NA04] National Security Agency. Information Assurance Technical Framework. Release 3.1. September 2002

[NA05] National Security Agency. The 60 Minute Network Security Guide: First Steps Toward a Secure Network Environment. Retrieved March 2004 from http://nsa2.www.conxion.com/support/guides/sd-7.pdf

[NE01] NetScreen Technologies, Inc.(2003, March). *Defense in Depth: A Strategy to Secure Federal Networks*. Retrieved January 2, 2003 from http://www.spectrum-systems.com/netscreen_federal.pdf

[NE02] http://www.networkcomputing.com/1214/1214ws1.html November 2003.

[OF01]Office of the Assistant Secretary of Defense: Command, Control, Communications, and Intelligence. DOD CIO Annual Information Assurance Report. April 2000 Retrieved November 2003 from http://www.defenselink.mil/nii/org/sio/ia/diap/documents/PUBLIC_CIO_IA-AnRpt_1999.pdf

[OM01]http://www.omnitechcorp.com/solutions/pdf/Basics%20of%20Intrusion%20Detection.pdf December 2003.

[PC01] http://www.pctechnicians.ca/ports.html February 2004.

[PE01] http://www.pestpatrol.com/Support/About/About_Ports_And_Trojans.asp February 2004.

[PR01] Proctor, Paul. Ask the Expert. CIO Magazine. Retrieved January 26, 2004 from http://www2.cio.com/ask%5Cexpert/2002/questions/question1516.html

[RA01] Ralston, Joseph. Memorandum for Distribution List; Subject Information Operations Condition. March 1999.

[RA02] Ralston, Joseph. Enclosure INFORMATION OPERATIONS CONDITION (INFOCON) March 1999.

[RO01] Rosenblatt, W (1993). *Learning the Korn Shell*. Sebastopol: O'Reilly.

[SANS00] http://isc.sans.org/infocon.html November 2003.

[SANS01] http://www.sans.org/resources/errors.php November 2003.

[SANS02] http://www.sans.org/resources/mistakes.php January 2004.

[SANS03] http://www.sans.org/rr/papers/8/659.pdf December 2003.

[SANS04] http://www.sans.org/rr/papers/index.php?id=525 January 2004.

[SANS05] http://www.sans.org/rr/papers/index.php?id=528 January 2004.

[SANS06] http://www.sans.org/rr/papers/index.php?id=594 January 2004.

[SANS07] http://www.sans.org/rr/papers/index.php?id=655 January 2004.

[SANS08] http://www.sans.org/rr/papers/index.php?id=1106 January 2004.

[SANS09] http://www.sans.org/rr/papers/index.php?id=1224 January 2004.

[SANS10]http://www.sans.org/rr/papers/index.php?id=1254 January 2004.

[SANS11] http://www.sans.org/rr/papers/index.php?id=1308 January 2004.

[SC01] http://www.scmagazine.com/scmagazine/sc-online/2002/article/27/article.html January 2004.

[SE01] http://www.securityfocus.com/infocus/1181 December 2003.

[SI01] http://www.simovits.com/nyheter9902.html February 2004.

[SS01] http://www.ssl.stu.neva.ru/psw/publications/crypto_eng.html January 2004.

[ST01] http://steve-parker.org/sh/hints.shtml February 2004.

[ST02] Stewart, Jack. JTF-CNO.

[ST03] http://www.stuffiveheard.com/tac/tacalerts.html December 2003.

[SY01] https://tms.symantec.com/threatCon_Def.asp December 2003.

[SY02] http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html January 2004.

[US01] http://www.uscg.mil/d5/group/GruEasternShore/cmdbrief/10-23_Command_Brief.ppt January 6, 2004.

[US02] http://www.usmchangout.com/id22.htm December 2003.

[WA01] http://www.washington.edu/computing/security/encryption.html January 2004.

[WE01] http://www.west-point.org/academy/malo-wa/educators/Threatcon.html December 2003.

[WH01] http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html January 2004.

[WW01] http://help.wwbcity.com/index.php?page=ports February 2004.

[ZA01] http://www.zakon.org/robert/internet/timeline December 2003.

[ZD01] http://www.zdnet.com.au/news/security/0,2000061744,20273490,00.htm January 2004.

[ZE01] http://www.zeltser.com/sans/gcfw-practical/perimeter_defense.pdf January 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. George Bieber
   OSD
   Washington, DC

4. RADM Joseph Burns
   Fort George Meade, MD

5. Deborah Cooper
   DC Associates, LLC
   Roslyn, VA

6. CDR Daniel L. Currie
   PMW 161
   San Diego, CA

7. LCDR James Downey
   NAVSEA
   Washington, DC

8. Richard Hale
   DISA
   Falls Church, VA

9. LCDR Scott D. Heller
   SPAWAR
   San Diego, CA

10. Wiley Jones
    OSD
    Washington, DC

11. Russell Jones
    N641
    Arlington, VA

12. David Ladd
Microsoft Corporation
Redmond, WA

13. Dr. Carl Landwehr
National Science Foundation
Arlington, VA

14. Steve LaFountain
NSA
Fort Meade, MD

15. Dr. Greg Larson
IDA
Alexandria, VA

16. Ray A. Letteer
Head, Information Assurance, HQMC C4 Directorate
Washington, DC

17. Penny Lehtola
NSA
Fort Meade, MD

18. Ernest Lucier
Federal Aviation Administration
Washington, DC

19. CAPT Sheila McCoy
Headquarters U.S. Navy
Arlington, VA

20. Dr. Ernest McDuffie
National Science Foundation
Arlington, VA

21. Dr. Vic Maconachy
NSA
Fort Meade, MD

22. Doug Maughan
Department of Homeland Security
Washington, DC

23. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

24. John Mildner
SPAWAR
Charleston, SC

25. Marshall Potter
Federal Aviation Administration
Washington, DC

26. Dr. Roger R. Schell
Aesec
Pacific Grove, CA

27. Keith Schwalm
Good Harbor Consulting, LLC
Washginton, DC

28. Dr. Ralph Wachter
ONR
Arlington, VA

29. David Wirth
N641
Arlington, VA

30. Daniel Wolf
NSA
Fort Meade, MD

31. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

32. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

33. Dr. George W. Dinolt
Naval Postgraduate School
Monterey, CA

34. J.D. Fulp
Naval Postgraduate School
Monterey, CA

35. Judy Pavina
Naval Postgraduate School
Monterey, CA

36. Paul Clark
Naval Postgraduate School
Monterey, CA

37. Jennifer Guild
Civilian, Naval Postgraduate School
Monterey, CA